ALFAMA CURSOS

alfamacursos.com.br

Alfama Cursos

Antônio Garcez
Fábio Garcez
Diretores Geral

Antônio Álvaro de Carvalho
Diretor Acadêmico

MATERIAL DIDÁTICO

Produção Técnica e Acadêmica

Patrícia Queiroz de Meneses
Coordenadora Geral

Patrícia Queiroz de Meneses
Coordenadora Pedagógica

Silvio Fernandes Menezes Vasconcelos
Walker Dantas Sampaio
Autoria

Gabriella Caroline Teles Silva
Sabina Regina Conceição Santos
Revisão Textual

Rafael Rezende de Farias
Editoração

Todos os direitos reservados e protegidos pela Lei 9.610 de 19/02/98.
É proibida a reprodução total ou parcial, por quaisquer meios, sem autorização prévia, por escrito, da ALFAMA CURSOS.

alfamacursos.com.br

Redes de Computadores

Apresentação do Curso

Nesta disciplina serão abordados temas pertinentes às tecnologias envolvidas na comunicação entre os computadores, fornecendo conhecimento necessário à compreensão das relações existentes entre o hardware e o software de rede, seus padrões e protocolos.

Por apresentar uma metodologia flexível, nossa proposta favorece o ritmo de aprendizagem de cada aluno. É preciso, no entanto, ficar atento aos prazos e ao planejamento pessoal para os estudos dos conteúdos e resolução das atividades avaliativas, para que vocês não se sobrecarreguem nem percam o ritmo de estudo.

Sucesso a todos!

Apresentação do Professor

SILVIO FERNANDES MENEZES VASCONCELOS é graduado em Informática, em Desenvolvimento de Aplicação Web pela Universidade Tiradentes e pós-graduando em Engenharia de Sistema. Possui experiência na área de Ciência da Computação, com ênfase em Desenvolvimento de Aplicação Web, atuando principalmente nos seguintes temas: Java, Aplicação Web e Banco de Dados. Na educação a distância trabalha como professor pesquisador do curso técnico em informática do E-Tec Sergipe.

WALKER DANTAS SAMPAIO é licenciado em Computação pelo Centro Universitário Claretiano de Batatais e pós-graduado em Educação a Distância pelo SENAC. Atualmente é professor/pesquisador do Projeto E-TEC Brasil, no estado de Sergipe. Possui experiência na área de Ciência da Computação, com ênfase em Processamento Gráfico, Programas de Escritório, Banco de Dados, Usabilidade, Arquitetura da Informação, Web Marketing, Ambientes Virtuais de Aprendizagem e Criação e Desenvolvimento para Web.

Componente Curricular

EMENTA:

Rede de Computadores, Tipos de Aplicações, Componentes de Redes, Topologia, Servidores, Arquitetura de Protocolo, Meio de Transporte, Interligando Segmento de Rede Local, Arquitetura TCP/IP, Protocolo TCP/IP, Endereçamento IP, Roteadores, Fundamentos de Redes Wan's, Modelo de Referência OSI, Meio Físico de Transmissão I, Meio Físico de Transmissão II, Padrões de Rede, Configuração de Rede Lógica, Política de Segurança, Sistema Operacional Windows NT, Sistema Operacional Linux, Linux x Windows NT, Futuro das Redes e Projeto de Redes.

HABILIDADES:

- Identificar meios físicos, dispositivos e padrões de comunicação, reconhecendo as implicações de sua aplicação no ambiente de rede.
- Analisar as características dos meios físicos disponíveis e as técnicas de transmissão digitais e analógicas fazendo relação entre os dois.
- Identificar os sistemas operacionais de redes, avaliando suas possibilidades em relação aos serviços e restrições.
- Identificar os principais tipos de tecnologias de arquitetura de rede, interpretando diagramas esquemáticos.
- Instalar os dispositivos de rede, os meios físicos e softwares desses dispositivos, analisando sua interconexão.
- Identificar as necessidades dos usuários em relação à segurança da rede conforme as políticas de acesso do ambiente em uso.

COMPETÊNCIAS:

- Identificar os diversos tipos de arquitetura de redes.
- Reconhecer os principais modelos de rede de comunicação entre sistemas de transmissão de dados, voz e imagem.
- Identificar os principais meios de comunicação web, utilizados em sistemas de pequeno, médio e grande porte.
- Instalar, configurar e operar redes do tipo Cliente/Cliente e Cliente/Servidor, com compartilhamento de recursos.

PÚBLICO-ALVO:

Estudantes de informática, técnicos de diversas áreas, empresas e repartições públicas.

Índice

Capítulo 1 - Rede de Computadores 11
1.1 – Introdução 11
1.2 – História 11
1.3 – Definição de Redes de Computadores 12
1.4 – Classificação de Redes 12
1.5 – Exercícios Propostos 15
Capítulo 2 - Tipos de Aplicações 16
2.1 – Introdução 16
2. 2 – Descrição 16
2.3 – Exercício Proposto 18
Capítulo 3 - Componentes de Redes 19
3.1 – Introdução 19
3.2 – Indrodução 19
3.3 – Cabo 19
3.4 – Hardware de Rede 20
3.4.1 – Servidores e Estação de Trabalho 20
3.4.2 – Dispositivos de Ligações 20
3.4.2.1 – Placa de Rede 20
3.4.2.2 – Placa de Rede ISA 20
3.4.2.3 – Placa de Rede PCI 21
3.4.2.4 – Hub 21
3.4.2.5 – Switch 21
3.4.2.6 – Roteador (Router) 22
3. 4.2.7 – Modem 22
3.5 – Software de Rede 22
3.6 – Exercícios Propostos 24
Capítulo 4 – Topologia 25
4.1 – Introdução 25
4.2 – Definição 25
4.2.1 – Topologia em Barra 25
4.2.2 – Topologia em Estrela 26
4.2.3 – Topologia em Anel 26
4.3 – Exercício Proposto 29
Capítulo 5 - Servidores 30
5.1 – Introdução 30
5.2 – Introdução 30
5.3 – Servidores de Arquivos 30
5.4 – Servidor de Impressão 31
5.5 – Servidor de Comunicação 31
5.6 - Servidor Gateway 32
5.7 – Servidor de Rede 32
5.8 – Exercício Proposto 33
Capítulo 6 - Arquitetura de Protocolo 34
6.1 – Introdução 34
6.2 - Nível Físico (ou Camadas) 34
6.3 – Nível de Ligação 34
6.4 - Nível de Rede 34
6.5 - Nível de Transporte 34
6.6 – Exercício Proposto 36
Capítulo 7 - Meio de Transmissão 37
7.1 – Introdução 37
7.2 – Par Trançado 37
7.3 – Cabo Coaxial 37
7.4 – Fibras Óticas 38
7.5 – Exercícios Propostos 39

Capítulo 8 - Interligando Segmento de Rede Local 40
8.1 – Introdução 40
8.2 – Repetidores 40
8.3 – Pontes 40
8.4 – Gateway 41
8.5 – Exercícios Propostos 42
Capítulo 9 - Arquitetura TCP/IP 43
9.1 - Introdução 43
9.2 - Camadas da Arquitetura 43
9.2.1 – Camadas de Aplicações 43
9.2.2 – Camadas de Transporte 44
9.2.3 – Camadas de Rede 44
9.2.4 – Camadas de Enlace de Rede 44
9.3 – Exercício Proposto 47
Capítulo 10 - Protocolo TCP/IP 48
10.1 – Introdução 48
10.2 – Protocolo da Arquiteruta TCP/IP 48
10.2.1 - Protocolo HTTP (Hypertext Transfer Protocol) 48
10.2.2 - Protocolo TELNET (Terminal Emulador) 49
10.2.3 - Protocolo FTP (File Transfer Ptotocol) 49
10.2.4 - Protocolo SMTP (Simple Mail Transfer Ptotocol)
E Pop (Post Office Protocol) 49
10.2.5 - Protocolo SNMP (Simple Network Management Protocol) 50
10.2.6 - Protocolo IP 50
10.2.7 - Protocolo ICMP 50
10.3 – Exercício Proposto 51
Capítulo 11 - Endereçamento IP 52
11.1 – Introdução 52
11.2 – Conceitos 52
11.3 – Classe de Endereço 52
11.4 – Classes Especiais 53
11.5 – Endereço de Rede 53
11 .6 – DHCP 53
11.7 – Exercício Proposto 55
Capítulo 12 – Roteadores 56
12.1 – Introdução 56
12.2 – Conceitos 56
12.3 – Protocolo de Roteamento 56
12.4 – Roteamento Estático e Dinâmico 57
Capítulo 13 - Fundamentos de Redes Wan's 58
13.1 – Introdução 58
13.2 – Conceitos 58
13.3 – Exercícios Propostos 60
Capítulo 14 - Modelo de Referência OSI 61
14.1 – Introdução 61
14.2 – Camadas do Modelo OSI 61
14.2.1 – Camada 7 – De Aplicação 62
14.2.2 – Camada 6 – De Apresentação 62
14.2.3 – Camada 5 – De Sessão 62
14.2.4 – Camada 4 – De Transporte 62
14.2.5 – Camada 3 – De Rede 63
14.2.6 – Camada 2 – De Enlace 63
14.2.7 – Camada 1 – De Física 63
14.3 – Exercício Proposto 64
Capítulo 15 - Meio Físico de Transmissão I 65
15.1 – Introdução 65
15.2 – Utilização dos Meios Físicos Guiados 65
15.3 – Tipos de Meios Físicos Guiados 65

15.3.1 – Par Trançado 63
15.4 – Exercícios Propostos 68
Capítulo 16 - Meio Físico de Transmissão II 69
16.1 – Introdução 69
16.2 – Utilização dos Meios Físicos Não Guiados 69
16.3 – Tipos de Meios Físicos Não Guiados 69
16.3.1 – Rádio, RF ou Radiofrequência 69
16.3.2 – Micro-ondas 70
16.3.3 – Laser 71
16.4 – Exercício Proposto 72
Capítulo 17 - Padrões de Rede 73
17.1 – Introdução 73
17.2 – Padrão IEEE 73
17.2.1 – IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z 74
17.2.2 – IEEE 802.11 74
17.2.3 – IEEE 802.16 75
17.3 – Exercício Proposto 76
Capítulo 18 - Configuração de Rede Lógica 77
18.1 – Introdução 77
18.2 – Rede Cliente/Servidor 77
18.3 – Rede Ponto a Ponto 77
18.4 – Exemplo de Configuração Lógica com o Windows XP 78
18.4.1 – Criando Conto do Usuário 78
18.5 – Exercício Proposto 80
Capítulo 19 - Política de Segurança 81
19.1 – Conceito 81
19.2 – Princípios de Segurança 81
19.3 - Tipos de Crackers 81
19.4 – Filosofias da Política 82
19.5 – Os Objetivos de Preoculpações 82
19.6 – Características da Boa Política 82
19.7 – Componentes da Boa Política 82
19.8 – Exercício Proposto 83
Capítulo 20 - Sistema Operacional Windows NT 84
20.1 – Introdução 84
20.2 – Característica do Software 84
20.3 – Característica do Hadware 84
20.4 – Família do Windows 85
20.5 – Exercício Proposto 86
Capítulo 21 - Sistema Operacional Linux 87
21.1 – Introdução 87
21.2 – Características 87
21.3 – Histórico 88
21.4 – Evolução do Ubuntu 88
21.5 – Exercícios Propostos 88
Capítulo 22 - Linux x Windows 89
22.1 – Introdução 90
22.2 – Windows 90
22.3 – Windows NT 90
22.4 – Linux 91
22.5 – Exercício Proposto 92
Capítulo 23 – Futuro das Redes 93
23.1 – Introdução 93
23.2 – IPv4 93
23.3 – IPv6 93
23.4 – Internet Via Rede Elétrica 94
23.5 – Exercício Proposto 95
Capítulo 24 -Projeto de Redes 96

24.1 – Introdução 96
24.2 – Requisitos 96
24.3 – Utilização 96
24.4 – Metodologia 96
24.5 – Exercícios Propostos 98
Referências 99

1 - REDE DE COMPUTADORES

1.1 – INTRODUÇÃO

Este capítulo inicial é para fornecer conhecimento da história, suas definições e classificação das redes de computadores. Vamos estudar como eles se comunicam e trocam dados de forma eficiente e segura, o que ocorre através das redes de computadores.

> *As redes de computadores existem para atender às demandas das aplicações comerciais, das aplicações domésticas e dos usuários móveis. Nas aplicações comerciais as redes são utilizadas principalmente para compartilhar recursos, como impressoras, arquivos e conexão com a Internet. Por que as pessoas compram computadores para usar em casa? No início, para processamento de textos e jogos, porém, nos últimos anos, esse quadro mudou substancialmente. Talvez agora a maior motivação seja o acesso à Internet. Alguns dos usos mais populares da Internet para usuários domésticos são: o acesso às informações remotas, a comunicação entre pessoas, o entretenimento interativo e o comércio eletrônico. (TANEMBAUM, 2003)*

Por fim, os usuários móveis, que utilizam seus celulares e notebooks para comunicação com fins domésticos ou comerciais.

1.2 – HISTÓRIA

> *As redes de computadores surgiram e evoluíram com a crescente necessidade de compartilhamento dos recursos computacionais e de informação nas empresas. As primeiras redes eram de pequeno porte, com poucos computadores interligados. Registra-se que um dos primeiros sistemas integrados de computadores começou a funcionar comercialmente nos Estados Unidos em 1964, para utilização nos serviços de reservas de passagens de companhias aéreas. Essas primeiras redes utilizavam soluções patenteadas de um único fabricante. (PINHEIRO, 2003)*

Na década de 1970 houve a primeira iniciativa para a implantação de uma rede de computadores de fabricantes diferentes. Naquela oportunidade, um grupo formado por empresas e entidades de padronização deu início ao movimento em direção ao que chamamos de protocolos abertos, ou seja, protocolos que não favoreciam uma única solução.

No início da década de 1980, a Xerox, a Digital e a Intel se uniram e foi lançado no mercado o padrão que veio impulsionar definitivamente o desenvolvimento das redes de computadores: o padrão Ethernet. (PINHEIRO, 2003)

Fica a dica

As redes Ethernet ou redes de arquitetura Ethernet são predominantes no mercado atual, com cerca de 90% do porque instalado em nível mundial. O sucesso se deu devido à padronização dos componentes que nelas são utilizados, garantindo altas taxas de transmissão e baixo custo.

1.3 – DEFINIÇÃO DE REDES DE COMPUTADORES

As redes de computadores são criadas para permitir a troca de dados entre diversos dispositivos – estações de trabalho, impressoras, redes externas, etc. – dentro de um determinado espaço físico, que pode ser uma área ou um segmento da própria rede.

> *Independente do tamanho e do grau de complexidade, o objetivo básico de uma rede é garantir que todos os recursos disponíveis sejam compartilhados rapidamente, com segurança e de forma confiável. Para tanto, uma rede de computadores deve possuir regras básicas e mecanismos capazes de garantir o transporte seguro das informações entre os elementos constituintes. (PINHEIRO, 2003)*

Uma rede de computadores vai muito além de uma simples conexão de cabos e placas de rede. Há necessidade de uma série de protocolos para regular a comunicação entre todos os níveis, desde o programa que está sendo utilizado até o tipo de cabo instalado.

Protocolo: são regras de padronização de procedimentos de modo que haja uma comunicação eficaz entre emissor e receptor. Por exemplo, ao conversar com uma pessoa usando a língua inglesa, é necessário que a outra pessoa compreenda a mesma língua. Assim, você estabelece que seu protocolo de comunicação verbal seja a língua inglesa. Todos os computadores se comunicam entre si através de protocolos.

1.4 – CLASSIFICAÇÃO DE REDES

As redes de computadores são classificadas de acordo com a dimensão geográfica que ocupam e todas elas são concebidas de forma que possam se comunicar com outras redes, assim, as redes podem ser classificadas em:

- **LAN (Local Area Network – Rede de Área local)**: este tipo de rede alcança distância de algumas centenas de metros, abrangendo instalações em escritórios, residências, prédios comerciais e industriais. Sua principal característica são as altas taxas de transmissão, que atualmente chegam a 10 gbps (porém, devido ao custo, ainda prevalecem as redes com taxas de transmissão de 100 Mbps a 1 gpbs).

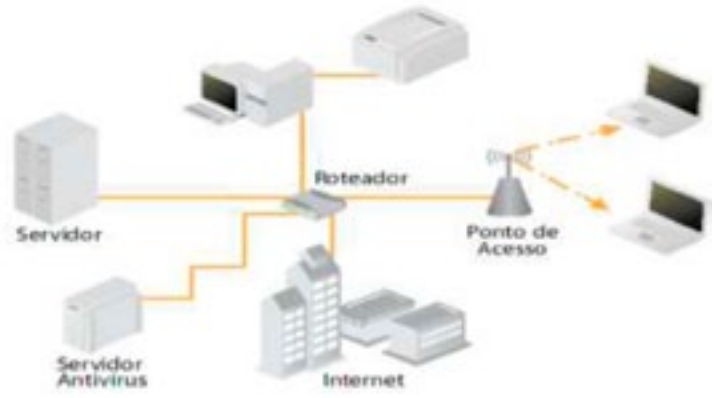

Figura 2 - Rede Local.

A rede LAN com interligação a uma rede wireless para os portáteis (notebooks) é mostrada também na figura 2. A rede tem dois servidores; o seu roteador (router) interliga a rede LAN propriamente dita (representada pelo microcomputador e multifuncional – impressora, scanner e fax) com a Internet e com o Ponto de Acesso (que permite o acesso sem fio).

A figura também pode exemplificar uma rede WLAN, já que o acesso sem fio pode ser caracterizado como uma rede WLAN. Neste tipo de rede (WLAN), as taxas de transmissão e as distâncias são menores, e as taxas de erro maiores.

• **MAN (Metropolitan Area Network – Rede de Área Metropolitana)**: abrange uma região com dimensões bem maiores do que as redes LAN, normalmente um campus de uma universidade, a instalação de uma fábrica e seus escritórios, ou até uma cidade inteira. Suas taxas de transmissão são inferiores e apresentam taxas de erros mais elevadas quando comparadas às redes LAN.

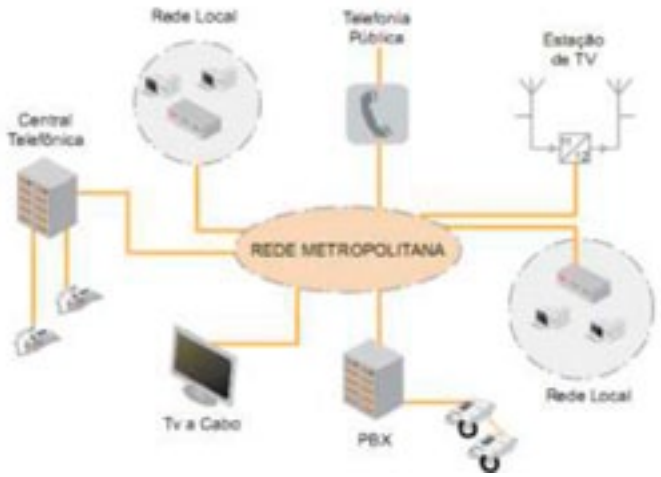

Figura 3 - Rede Metropolitana.

Podemos observar a interligação de vários subsistemas locais através de uma rede MAN. TV a cabo, redes locais (LAN) e sistemas públicos de telefonia são todos ligados por um enlace que pertence a uma rede Metropolitana. Figura 3.

A oferta de redes MAN é justificada pela necessidade que as empresas têm de se comunicar com localidades distantes. São as operadoras de telefonia que normalmente oferecem infraestrutura para este tipo de rede, cujo exemplo pode ser a comunicação entre Matriz e Filiais.

• **WAN (Wide Area Network – Rede de Área Extensa)**: é o conceito de rede extensa. Este tipo de rede tem dimensões geográficas imensuráveis. Isto quer dizer que ela pode interligar todos os continentes, países e regiões extensas utilizando enlaces mais extensos, como satélites ou cabos (submarinos ou terrestres). Tem baixas taxas de transmissão e altas taxas de erros. É normalmente utilizada para interligar redes MAN ou WMAN. O principal exemplo desta rede é a Internet, que interliga computadores do mundo inteiro. O conceito de WWAN surgiu devido à necessidade de interligar redes com enlaces sem fio a grandes distâncias. As redes de celulares podem ser consideradas exemplos de WWAN.

Com o surgimento das novas tecnologias de rede wireless (sem fio), novas classificações foram adotadas:

- WPAN (Wireless Personal Area Network – Rede sem fio de Área Pessoal).
- WLAN (Wireless Local Area Network – Rede sem fio de Área Local).
- WMAN (Wireless Metropolitan Area Network – Rede sem fio de Área Metropolitana).

- WWAN (Wireless Wide Area Network – Rede sem fio de Área Extensa).

Um novo conceito em redes sem fio são as WPAN. Como indica o P da sigla, essas são as redes pessoais. A tecnologia de comunicação das pessoas com os equipamentos evoluiu de modo a exigir uma padronização e a criação de uma nova tecnologia. Essa padronização possibilita ao usuário adquirir dispositivos de marcas diferentes e que se comunicam entre si. A tecnologia mais comum para WPAN é o Bluetooth, muito utilizado para troca de arquivos entre dispositivos móveis, como celulares e notebooks. Outro exemplo é o iR (InfraRed – infravermelho), que também pode ser considerado um WPAN.

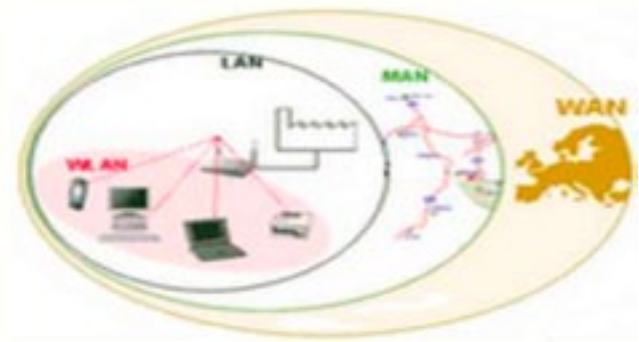

Figura 4 - Integração entre redes WAN, MAN e LAN.

As elipses estão uma dentro da outra como mostrado na figura 4, pois, normalmente, uma rede MAN abrange várias LAN's, assim como uma WAN pode abranger várias MAN's. Apesar de não aparecer escrito no diagrama, estão subentendidas as tecnologias de rede sem fio de cada classificação, WLAN, WMAN e WWAN.

Segue abaixo uma tabela que representa as características de cada tipo dentro da classificação adotada:

Classificação	Taxa de transmissão	Taxa de erros	Distâncias
WAN	Na ordem de 622 Mbps	Alta	Milhares de quilômetros
MAN	Na ordem de 2,5 Gbps	Média	Centenas de quilômetros
LAN	Na ordem de 10 Gbps	Baixa	Centenas de metros
WPAN	Na ordem de 1 Mbps	Baixa	Dezenas de metros

1.5 – EXERCÍCIOS PROPOSTOS

1) Escreva com suas palavras, o que você entende por Rede de Computadores.

_____
_____
_____

2) Como são classificadas as Redes de Computadores?

_____
_____
_____

2 - TIPOS DE APLICAÇÕES

2.1 – INTRODUÇÃO

Neste capítulo iremos falar sobre as aplicações utilizadas nas redes de computadores, quanto à cobertura geográfica, tráfego, confiabilidades, as transmissões de dados e seus tipos de interação com outros dispositivos ligados à rede. Vamos estudar como funcionam esses tipos de aplicações em uma rede de computadores local.

2.2 – DESCRIÇÃO

As redes locais têm em geral três domínios de aplicações quanto à cobertura geográfica: uma única sala (por exemplo, para compartilhamento de dispositivos especiais entre vários computadores), dentro de um edifício (por exemplo, na integração de um serviço de escritório), ou mesmo uma área coberta por vários edifícios (por exemplo, um campus universitário, uma fábrica, ou uma pequena cidade). A dispersão geográfica, como veremos, é fundamental na escolha da topologia e do meio de transmissão, sendo um fator importante também em alguns tipos de protocolo.

O ambiente de operação influencia também na escolha do meio de transmissão e topologia. Ambientes ruidosos e com problemas de segurança têm requisitos mais fortes quanto à escolha. A ocorrência de erros devido a ruídos exigirá também dos protocolos, mecanismos de detecção e recuperação em alguns casos.

O número máximo de nós, a separação máxima e mínima entre nós e a taxa máxima de informação transmitida, também influenciam na escolha do meio de transmissão e na topologia da rede. Em alguns tipos de topologia, a ligação ao meio de transmissão é outro fator limitante ao número de nós que uma rede pode suportar à separação máxima e mínima entre eles. A escolha do protocolo de acesso é também diretamente influenciada por estes fatores. Alguns protocolos, por exemplo, leva em conta a distância máxima entre nós para seu perfeito funcionamento.

A exigência de tempo de resposta máximo limitado bem como o tipo de tráfego exigido será de fundamental importância na escolha do protocolo de acesso. Para aplicações de controle de processos e outras aplicações em tempo real, a garantia de tempo de resposta limitada é uma característica desejável. Infelizmente, em qualquer aplicação existe sempre uma possibilidade de um erro de transmissão, que causará uma não limitação no tempo de resposta em qualquer caso. Em muitas aplicações, entretanto, é importante que este problema não seja causado pelo tipo de protocolo utilizado.

O tráfego em geral varia desde rajadas de alguns dados de grandes mensagens até quantidades volumosas de dados sendo transmitidos continuamente, como é o caso de algumas aplicações que exigem a comunicação ao computador. A confiabilidade exigida será fundamental tanto na escolha do meio de transmissão, quanto na topologia e no protocolo de acesso.

O tipo de informação transmitida pode ser dados, vídeo e voz. Os diversos tipos de transmissão vão diferir em termos de frequência, quantidade de informação transmitida, natureza analógica ou digital, requisitos de tempo real e de isenção de erros, etc. Transmissão de dados entre dispositivos em geral deve ser isenta de erros requerendo retransmissão através da estrutura do protocolo, quando estes erros são detectados. Transmissão de voz e vídeo, em geral, deve ser efetivada sem interrupção em tempo real e tem uma tolerância a erros, até certo ponto. Integração de tráfegos heterogêneos em um sistema comum é desejável por razões econômicas e pela simplicidade de operação. Integração vai oferecer a possibilidade de um compartilhamento dinâmico das facilidades de transmissão e de

chaveamento, além de dar suporte às novas aplicações, tais como teleconferência, que requer acesso aos diferentes tipos de informação: voz, dados e vídeo. O tipo de informação transmitida será determinante na escolha do meio de transmissão e do protocolo à rede, podendo chegar ao ponto de exigir circuitos dedicados para comunicação ponto a ponto.

O tipo de interação entre dispositivos impõem diferentes requisitos à rede. Aplicações para comunicação computador/terminal são geralmente orientadas a transações com tráfego do tipo rajada. O envolvimento de operadores humanos exige um serviço do tipo conversacional com velocidade razoavelmente baixa. O objetivo maior desta aplicação é fornecer aos usuários de terminais geograficamente dispersos, acesso aos bancos de dados e à fonte computadora. Aplicações para comunicação computador/computador (transferências de arquivos, processamento distribuído, etc.) exigem velocidade de comunicação maior, e possuem um tráfego mais intenso, algumas vezes regular.

2.3 – EXERCÍCIO PROPOSTO

1) Quais são os três domínios de aplicações quanto à cobertura geográfica?

_____
_____
_____

3 - COMPONENTES DE REDES

3.1 – INTRODUÇÃO

Com o acréscimo das tecnologias de transmissão e os equipamentos evoluindo rapidamente, precisamos saber quais equipamentos que tornarão possível a criação das redes. Neste capítulo iremos estudar sobre os novos hardwares de rede e depois abordaremos o software necessário para o funcionamento do mesmo.

3.2 – INDRODUÇÃO

Uma rede é um grupo de computadores ligados entre si para efeitos de compartilhamento de informações um com o outro. Embora as redes tenham sido usadas em ambientes de negócios durante muitos anos, agora estão se tornando cada vez mais comuns nas casas como um meio de partilhar ligação à Internet. Uma rede de computador tem várias partes diferentes e cada uma tem sua própria finalidade.

3.3 – CABO

> *Com o crescimento da tendência de interligação entre as redes de computadores e os diversos sistemas de comunicação e automação existentes, como as redes de telefonia, os sistemas de segurança, os sistemas de administração predial, etc. Essa junção de tecnologias vai mudar a maneira como os ambientes de trabalho são concebidos nas empresas e mesmo em nossas casas. A infraestrutura básica para essas novas tecnologias são os Sistemas de Cabeamento Estruturado – SCS (Structured Cabling System). (PINHEIRO, 2003)*

Cabeamento Estruturado é um conceito que redefine a forma como os cabos de dados são utilizados nas empresas e nas residências. Tem como objetivo manter a rede física organizada e padronizada, com o uso de conectores e cabos com desempenho satisfatório para o fim a que se aplica. Seu layout permite a instalação de equipamentos como servidores, computadores e demais acessórios de rede com alto grau de organização e confiabilidade.

Segundo Pinheiro (2003), diz que cerca de 70% dos problemas da rede estão associados ao cabeamento que ela utiliza. Entretanto, na maioria das pequenas redes, ainda é predominante o uso do cabeamento não estruturado.

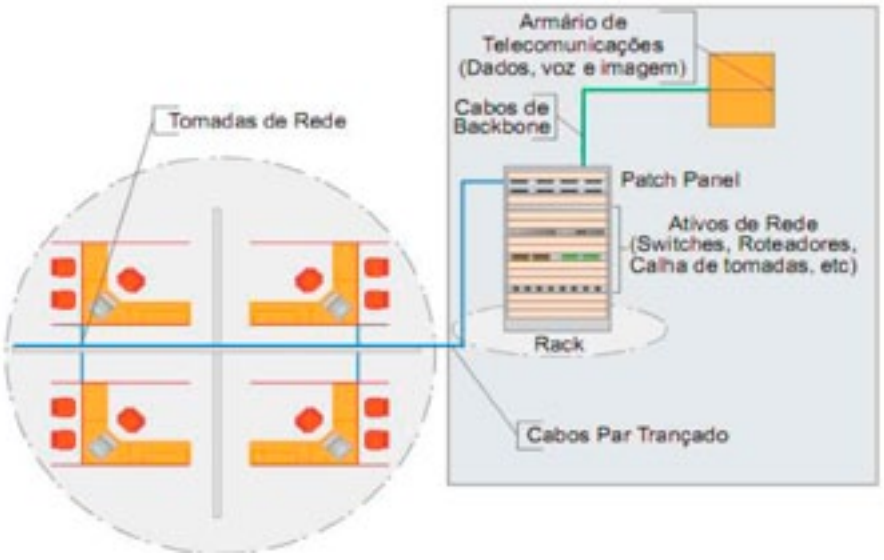
Armário de Telecomunicações (Dados, voz e imagem)
Cabos de Backbone
Tomadas de Rede
Patch Panel
Ativos de Rede (Switches, Roteadores, Calha de tomadas, etc)
Rack
Cabos Par Trançado

Figura 5 - Cabeamento Estrutura.

Observe que a área de trabalho conectada através de cabos estruturados de rede, como na figura 5, onde existem elementos como: tomadas de rede, rack (que agrupa os equipamentos), cabos de par trançado e cabos de backbone (que têm função de transportar grandes volumes de informações da rede).

3.4 – HARDWARE DE REDE

Assim como os computadores possuem hardware específico para funcionar (placas, processadores, memórias...), as redes também precisam de componentes específicos. Esses componentes são chamados de hardware de rede e são responsáveis por conectar equipamentos em sua rede local ou de longa distância. Os exemplos mais simples são: a placa de rede do seu computador ou o chip bluetooth do seu celular.

3.4.1 – SERVIDORES E ESTAÇÃO DE TRABALHO

Esses dois itens são apenas computadores que formam a rede. Entretanto, como eles fornecem serviços de comunicação, poderão ser catalogados aqui como hardware de rede.

1. Servidores: normalmente são computadores destinados a prestar serviços aos outros (às estações de trabalho). Pode-se dizer que qualquer PC pode ser um servidor de rede, mas normalmente são computadores mais potentes, com muita capacidade de memória e de armazenamento (discos rígidos maiores).

2. Estação de Trabalho: normalmente são os computadores clientes da rede, neles os usuários rodam seus programas e acessam os serviços fornecidos pelo servidor. São computadores mais simples, com pouca ou nenhuma redundância, possuem também menos memória e menos capacidade de armazenamento.

3.4.2 – DISPOSITIVOS DE LIGAÇÕES

São os componentes (dispositivos) necessários para construir uma rede local.

3.4.2.1 – PLACA DE REDE

Uma placa de rede é um dispositivo de hardware responsável pela comunicação entre os computadores de uma rede. A placa de rede é o hardware que permite aos computadores conversarem entre si através da rede. A sua função é controlar todo o envio e recepção de dados através da rede.

Figura 6 - Placa de Rede.

3.4.2.2 – PLACA DE REDE ISA

- A comunicação das placas de rede ISA chega a 10 Mbps.
- É utilizado para conectar periféricos lentos, como a placa de som e fax modem (16 bits - baixa velocidade).
- Fora de linha, são utilizadas nos computadores antigos.

Figura 7 - Placa de Rede ISA.

3.4.2.3 – PLACA DE REDE PCI

- A comunicação em placas de rede PCI pode atingir até 100 Mbps.
- Utilizada por periféricos que demandem velocidade, como a placa de vídeo (32 bits - alta velocidade).

Figura 8 - Placas de Rede PCI.

3.4.2.4 – HUB

É um dispositivo que tem a função de interligar os computadores de uma rede local. A forma como trabalha é a mais simples que a do Switch e o Router. O Hub recebe dados vindos de um computador e transmite-os para outras máquinas. No Hub é possível ter várias portas, que são as entradas que conectam o cabo de rede de cada computador. Geralmente há aparelhos com 8, 16, 24 e 32 portas. Este dispositivo utiliza a topologia em estrela.

Figura 9 – Hub.

3.4.2.5 – SWITCH

É um dispositivo utilizado em redes de computadores para reencaminhar módulos entre os diversos nós. Possuem portas assim como o Hub. Este dispositivo utiliza a topologia em

anel.

Figura 10 – Switch.

3.4.2.6 – ROTEADOR (ROUTER)

É um equipamento usado para fazer a computação de protocolos, a comunicação entre diferentes redes de computadores provocando a comunicação entre computadores distantes entre si. Os routers mais modernos necessitam de um cabo de banda larga ligado a um modem como entrada.

Figura 11 – Router.

3.4.2.7 – MODEM

É um dispositivo eletrônico que modula um sinal digital numa onda analógica, pronta para ser transmitida pela linha telefônica, e que demodula o sinal analógico e reconverte-o para o formato digital original. Utilizado para conexão à Internet ou a outro computador.

Figura 12 – Modem.

3.5 – SOFTWARE DE REDE

Em diferentes níveis de aplicação, os softwares de rede existem para gerenciar as comunicações entres os computadores conectados numa rede, por exemplo, o próprio comunicador instantâneo (como MSN ou MIRC) é um tipo de software para funcionar em

rede. Entre esses softwares, basicamente podemos destacar:

- Sistema Operacional de Rede (SOR).
- Aplicativos para rede, como antivírus, MSN, etc.
- Software de segurança e acesso à rede.

Os SOR's são programas que têm duas funções. A primeira é funcionar como um sistema operacional comum, fazendo o controle dos recursos do computador/servidor, como o acesso a disco rígido ou memória. A segunda função é fazer o controle do uso das redes que estão instaladas, por exemplo, como o usuário da rede pode ter acesso a um arquivo no disco rígido do servidor ou não. Os SOR's têm duas classificações, são elas: PONTO A PONTO e CLIENTE/SERVIDOR.

- **PONTO A PONTO:** nessas redes, os sistemas operacionais instalados em todos os computadores são do tipo cliente. Não é definido um computador específico para controle dos recursos da rede, como uma impressora, por exemplo. Os SOR's mais comuns são atualmente o Windows XP Professional Edition, o Windows Seven e as distribuições do Linux como Kurumim, Mandriva e Ubuntu. Esses SOR's configurados corretamente permitem aos computadores trocar dados através de redes cabeadas ou sem fio. Os seus problemas são a organização e segurança, pois fica tudo mais difícil de controlar, já que não existe a figura de um servidor que controle o acesso aos recursos da rede. Um ponto positivo é a sua facilidade de instalação e de configuração, que não exigem suporte técnico muito especializado.
- **CLIENTE/SERVIDOR:** nessas redes, os sistemas operacionais são SOR Cliente ou SOR Servidor. Os computadores clientes possuem sistemas operacionais do tipo cliente, os mesmos usados nas redes ponto a ponto; eles solicitam aos servidores os serviços ou recursos da rede, como arquivos, impressoras e internet. Os servidores executam um SOR Servidor, como por exemplo, o Windows 2003 Server, o Windows 2008 Server ou as distribuições Linux para servidores. Esses servidores permanecem todo o tempo executando serviços e atendendo às solicitações dos clientes, e um exemplo de serviço é a autenticação dos usuários que querem entrar na rede, assim, a rede se torna mais segura, pois podem ser rastreados os momentos e a estação na qual o usuário se autenticou. Essas redes são mais complexas e mais caras, pois necessitam de um Software Servidor e pessoal técnico qualificado para instalar e manter os serviços oferecidos pelo servidor.

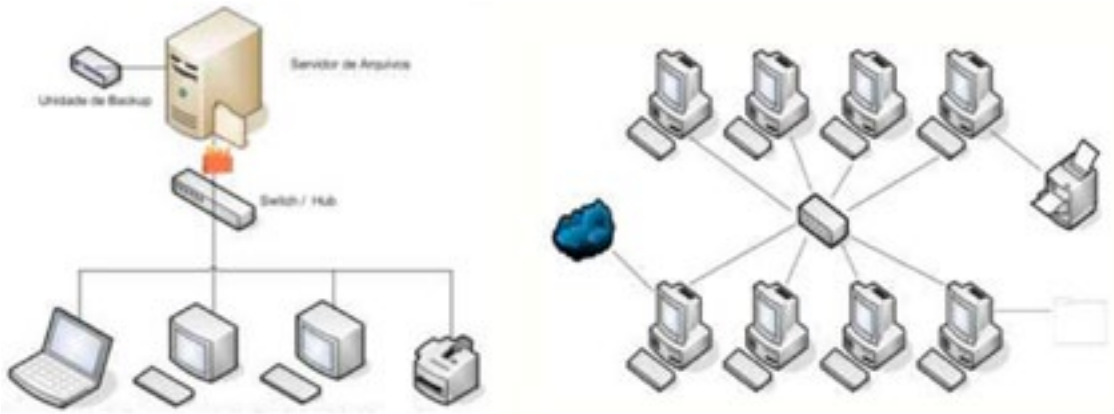

Figura 13 - Redes Cliente/Servidor e Ponto a Ponto.

3.6 – EXERCÍCIOS PROPOSTOS

1) Descreva pelo menos três tipos de dispositivos de ligação e para que servem.

_____
_____
_____

2) Quais são as duas classificações dos SOR's?

_____
_____
_____

4 – TOPOLOGIA

4.1 – INTRODUÇÃO

Neste capítulo iremos estudar as topologias de rede, sua definição e os vários tipos de topologia de rede que existem para criar uma rede de computadores local.

4.2 – DEFINIÇÃO

Conforme definido, as Redes Locais constituem-se de um conjunto de estações (nós) interligadas por um sistema de comunicação. Este sistema se comportará de um arranjo topológico interligando os vários nós e de um conjunto de regras de forma a organizar a comunicação. Dentre as topologias mais usadas encontram-se a estrela, o anel e a barra comum. Os equipamentos ligados em rede, para trocar informações entre si, necessitam que algum meio físico os conecte, um cabo de algum material ou o próprio ar, no caso de redes sem fio. Daí surge o conceito de topologia de rede, cuja classificação abrange, basicamente: Barramento, Estrela e Anel.

4.2.1 – TOPOLOGIA EM BARRA

Topologia em barra comum se caracteriza pela ligação de estações (nós) ao mesmo meio de transmissão. A barra é geralmente compartilhada no tempo ou na frequência, permitindo a transmissão de informação. Ao contrário das outras topologias que são configurações ponto a ponto (isto é, cada enlace físico de transmissão conecta apenas dois dispositivos), a topologia em barra tem uma configuração multiponto (isto é, mais de dois dispositivos estão conectados ao meio de comunicação).

Figura 14 - Uma topologia física em barra.

Entretanto, podemos observar na figura 14 todas as estações interconectadas por um barramento. Tecnicamente falando, existe uma série de conectores específicos para interligar cada computador ao barramento.

Nas redes em barra comum cada nó conectado à barra pode ouvir todas as informações transmitidas. Existe uma variedade de mecanismos para o controle de acesso à barra, que pode ser centralizado ou descentralizado. A técnica adotada para cada acesso à rede (ou a banda de frequência de rede no caso de redes em banda larga) é a multiplexação no tempo. Em um controle centralizado, o direito de acesso é determinado por uma estação especial da rede.

O desempenho de um sistema em barra comum é determinado pelo meio de transmissão, como o número de nós conectados, o controle de acesso, o tipo de tráfego e outros fatores.

Por empregar interfaces passivas, a inexistência de armazenamento local de mensagens e a inexistência de retardos no repetidor não vão degradar o tempo de resposta, que, contudo, pode ser altamente dependente do protocolo de acesso utilizado.

Em um ambiente de controle descentralizado, a responsabilidade é distribuída entre todos os nós. Do ponto de vista do desempenho, as redes com essa topologia eram muito instáveis, pois qualquer defeito em algum conector ou em alguma parte do cabo fazia com que toda a rede parasse.

4.2.2 – TOPOLOGIA EM ESTRELA

Neste tipo de topologia cada nó é interligado a um nó central (mestre), através do qual todas as mensagens devem passar. Tal nó age, assim, como centro de controle da rede, interligando os demais nós (escravos) que usualmente podem se comunicar apenas com outro nó de cada vez. Isto não impede que haja comunicações simultâneas, desde que as estações envolvidas sejam diferentes. Esses equipamentos concentradores são atualmente denominados Hubs e Switches. O cabeamento também evoluiu, passando do coaxial (utilizado na topologia de barra anteriormente) ao par trançado (o mais utilizado nas topologias atuais). Quase todas as redes locais instaladas atualmente utilizam esta topologia devido às facilidades e taxas de transmissão que ela oferece.

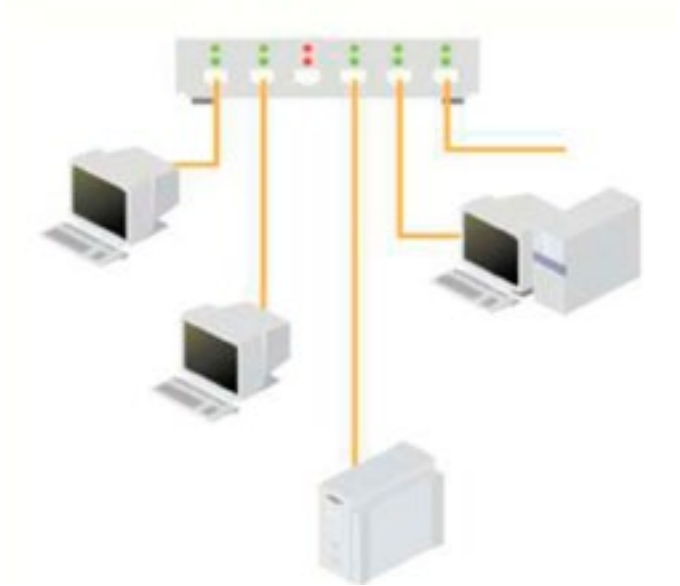

Figura 15 - Uma topologia física em estrela.

Na figura 15 pode-se observar que há no centro um aparelho concentrador (hub ou switch) que interconecta todos os cabos que vêm dos computadores (nós). Ainda há a saída de um cabo, cujo destino ou origem não está definido na figura. Ele pode estar ligado a algum outro tipo de concentrador, como por exemplo, um roteador que oferece conexão com a internet ou outro switch, criando outra rede com mais computadores interligados.

Várias redes em estrela operam em configurações onde o nó central tem tanto a função de gerência de comunicação, como as facilidades de processamento de dados. Em outras redes, o nó central tem como única função o gerenciamento das comunicações. Confiabilidade é um problema nas redes em estrela. Falhas em um nó escarvo apresentam um problema mínimo de confiabilidade, uma vez que o restante da rede ainda continua em funcionamento. Falhas no nó central, por outro lado, podem ocasionar a parada total do sistema. Redundâncias podem ser acrescentadas, porém as dificuldades de custo em tornar o nó central confiável pode mais do que mascarar o benefício obtido com a simplicidade das interfaces exigidas pelas estações secundárias.

4.2.3 – TOPOLOGIA EM ANEL

Uma rede em anel consiste de estações conectadas através de um caminho fechado, evitando os problemas de confiabilidade de uma rede em estrela. O anel não interliga as estações diretamente, mas consiste de uma série de repetidores ligados por um meio físico, sendo cada estação ligada a estes repetidores.

Redes em anel são capazes de transmitir e receber dados em qualquer direção. As configurações mais usuais, no entanto, são unidirecionais. O projeto dos repetidores mais simples é tornar menos sofisticados os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em sequência ao destino, pois sendo unidirecional evita o problema do roteamento. Os repetidores são, em geral, projetados de forma a transmitir e receber dados simultaneamente, diminuindo assim o retardo de transmissão e assegurando um funcionamento do tipo "full-duplex".

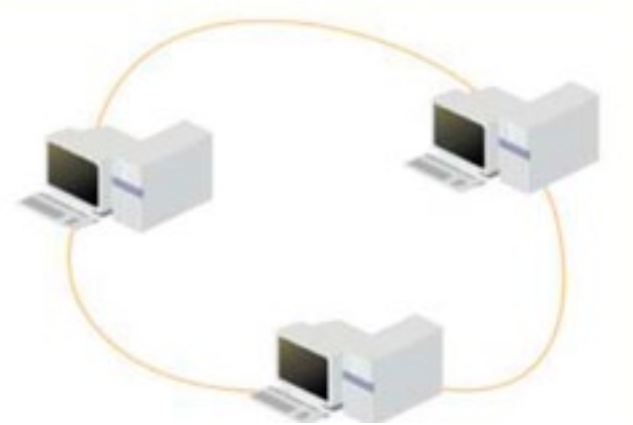

Figura 16 - Uma topologia física em anel.

Esta rede possui uma característica interessante, que é a recuperação de falhas, pois a comunicação entre os nós da rede pode ser feita no sentido horário ou anti-horário. Isso se deve a uma configuração automática realizada na instalação. Essas redes se tornaram, entretanto, inviáveis devido à dificuldade de inserção de novos nós na rede, à quantidade de falhas e ao seu custo.

Quando uma mensagem é enviada por um nó, ela entra no anel e circula até ser retirada pelo nó de destino, ou então até voltar ao nó fonte, dependendo do protocolo empregado. Os maiores problemas com topologia em anel são sua vulnerabilidade a erros e pouca tolerância a falhas. Qualquer que seja o controle de acesso empregado, ele pode ser perdido por problemas de falhas e pode ser difícil determinar com certeza se este controle foi perdido ou decidir qual nó deve recriá-lo. Erros de transmissão e processamento podem fazer com que uma mensagem continue eternamente a circular no anel.

Na figura 17 mostra atualmente as topologias fundidas, formando o que chamamos de topologias mistas, com grande predominância da estrela.

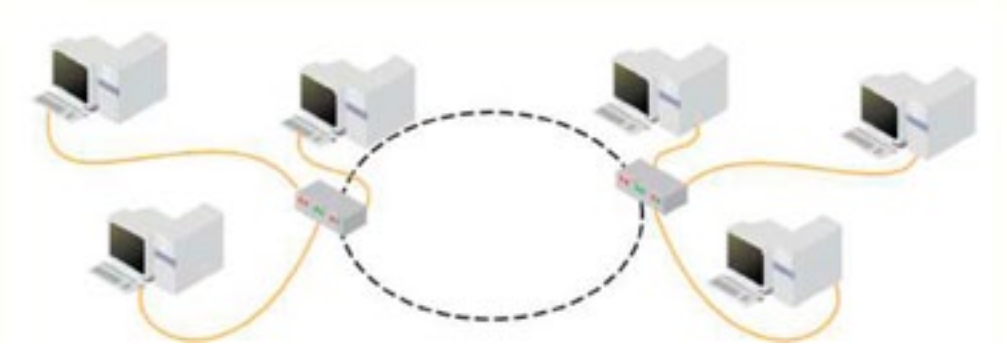

Figura 17 - Uma topologia mista.

Nesta figura há uma mistura de topologia anel (ligação central) com estrela (nas extremidades). Como há uma ligação dupla entre os dois concentradores, a tendência é utilizar apenas uma via para transmissão entre as redes, deixando a outra como reserva, isso é possível graças à evolução dos equipamentos, que permitem que as redes funcionem mesmo em condições de falhas, tornando mais eficiente a organização, que não precisa parar para que seja feita a manutenção. Tais equipamentos são utilizados mais por empresas do que por usuários domésticos, pois os custos de aquisição e manutenção destes aparelhos são mais elevados.

4.3 – EXERCÍCIO PROPOSTO

1) Descreva os tipos de topologias de rede de computadores?

_____
_____
_____

5 - SERVIDORES

5.1 – INTRODUÇÃO

Neste capítulo iremos falar sobre servidores, bem como os tipos de servidores que podem ser utilizados em sua rede de computadores, tais como, Servidores de Arquivos, Servidores de Impressão, Servidores de Comunicação, Servidores Gateway e Servidores de Rede.

5.2 – INTRODUÇÃO

Uma das funções básicas das redes locais é o compartilhamento de recursos caros e especializados (quer equipamentos, programas, base de dados, ou vias de comunicação), isto é: serviços, entre os vários usuários da rede.

Qualquer estação de uma rede local (servidores) pode oferecer serviço a outras estações (clientes). Vários serviços são típicos para cada aplicação e estações de propósito específicas são projetadas de forma a melhor oferecê-los. Tais servidores são distinguidos das outras estações apenas pelo software que os suportam e algum hardware especial que contenham. Entre os serviços mais oferecidos podemos citar: o armazenamento de arquivos, a gerência de banco de dados, o suporte para impressão, a tradução de nomes simbólicos em endereços físicos, concentrador de terminais, o suporte a telex, a monitoração de redes, a criptografia, o correio eletrônico, o suporte teletext, os Gateways para outras redes e outras funções de hardware e software.

Servidores podem ser também clientes de outros servidores da rede. Por exemplo, o servidor de impressão pode ser cliente de um servidor de arquivo ao fornecer serviços aos seus próprios clientes. Serviço de correio eletrônico é outro exemplo de servidor que muitas vezes é realizado utilizando os serviços de armazenamento de arquivos de outro servidor.

5.3 – SERVIDORES DE ARQUIVOS

O Servidor de Arquivo tem como função oferecer aos seus clientes o serviço de armazenamento e acesso às informações de compartilhamento de disco. Controlam unidades de disco ou outras unidades de armazenamento, sendo capazes de aceitar pedidos de transações das estações clientes e atendê-los utilizando os seus dispositivos de armazenamento.

Um Servidor de Arquivo Geral é aquele que é capaz de aceitar transações independentes do sistema operacional do cliente, ou seja, independente da estrutura de arquivos da estação cliente. Neste caso, existe um sistema de arquivo padrão da rede, utilizado pelo servidor de arquivos, nos quais os vários arquivos das demais estações da rede devem ser convertidos (pelos protocolos no nível de apresentação) para comunicação com o Servidor. Sendo adotada esta solução, todos os arquivos da rede são potencialmente acessíveis a todas as estações, independente das estruturas de arquivos individuais.

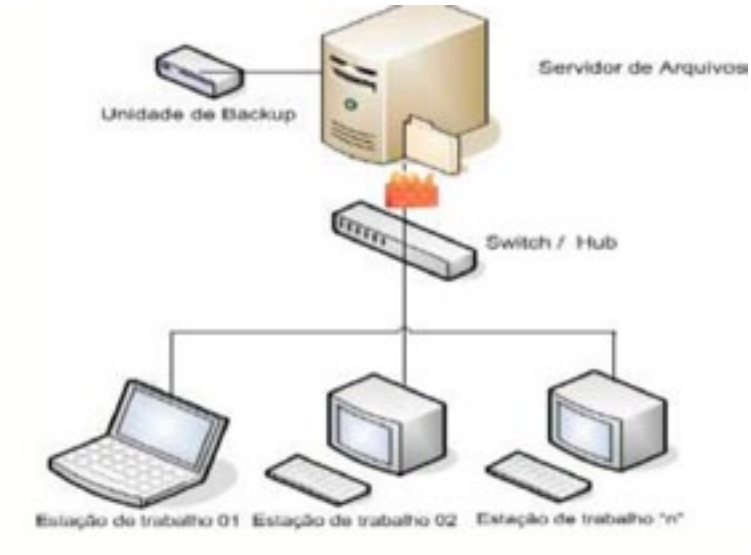

Figura 18 - Servidor de Arquivo.

5.4 – SERVIDOR DE IMPRESSÃO

O Servidor de Impressão tem como finalidade oferecer serviços de impressão aos seus clientes. Um Servidor de Impressão típico tem vários tipos de impressoras acopladas, cada uma adequada à qualidade ou rapidez de uma aplicação particular.

Existem várias formas de se implementar um Servidor de Impressão. A forma mais simples é baseada na pré-alocação da impressora. Neste caso, uma estação cliente envia um pedido ao Servidor, manifestando o desejo de uso de uma impressora específica. Caso esta impressora esteja disponível, ela então é alocada ao cliente até que este a libere (ou, então, até que se esgote o tempo máximo da utilização, conforme negociação na alocação). Caso a impressora não esteja disponível, o cliente é avisado e colocado em uma fila de espera.

Outra forma de implementar um Servidor de Impressão é utilizando a técnica de "spooling". Neste caso, a estação ao invés de pedir a alocação de uma impressora, envia diretamente ao Servidor o texto a ser impresso. Este texto é colocado em uma fila de espera, sendo impresso quando a impressora estiver disponível.

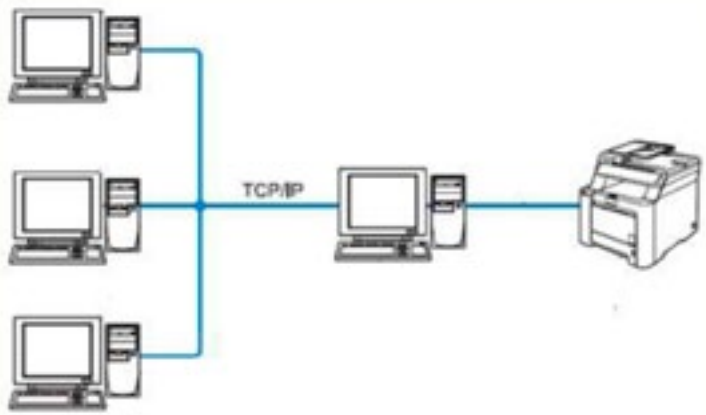

Figura 19 - Servidor de Impressão.

5.5 – SERVIDOR DE COMUNICAÇÃO

Consiste em uma estação especial de frente que será responsável pela realização de todos os procedimentos de acesso à rede, bem como da interface com os dispositivos dos

usuários, de forma a permitir o uso da rede por estes.

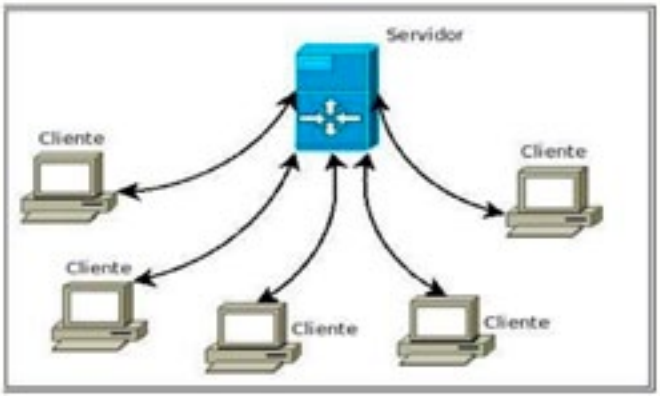

Figura 20 - Servidor de Comunicação.

5.6 - SERVIDOR GATEWAY

São estações da rede que oferecem serviço de comunicação com outras redes para seus clientes. A ligação entre redes pode ser realizada via repetidores ou pontes, mas quando se trata de interligação de redes distintas, o uso de Gateway se torna indispensável.

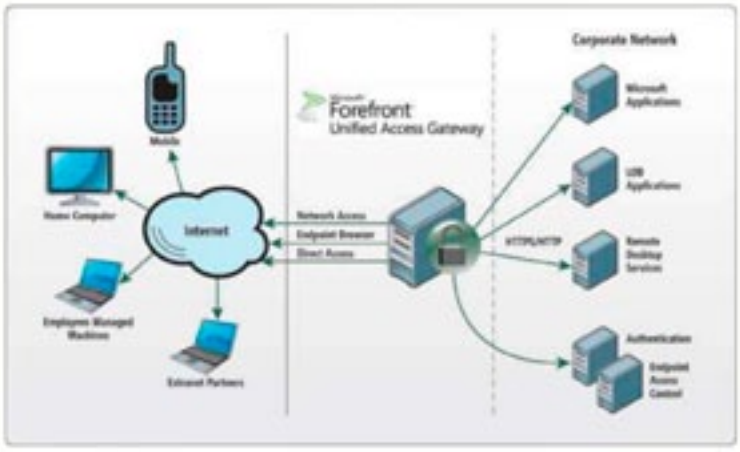

Figura 21 - Servidor de Gateway.

5.7 – SERVIDOR DE REDE

Monitoração do tráfego, do estado, do desempenho de uma estação da rede, assim como a monitoração do meio de transmissão e outros sinais são necessários para o gerenciamento da rede, de forma a possibilitar a detecção de erros, diagnose e resoluções de problemas da rede, tais como falhas, desempenho e etc.

Figura 22 - Servidor de Rede.

5.8 – EXERCÍCIO PROPOSTO

1) Escreva pelo menos cinco servidores e suas utilizações.

_____
_____
_____

6 - ARQUITETURA DE PROTOCOLO

Neste capítulo teremos uma visão geral do modelo de protocolo e seus níveis de comunicação dos dados que são transmitidos pela rede, tais como, nível físico, nível de ligação, nível de rede e nível de transporte.

6.1 – INTRODUÇÃO

O objetivo de uma estrutura de protocolo em níveis é delimitar e isolar funções de comunicação a camadas.

Os dados transferidos em uma comunicação de um dado nível não são enviados diretamente (horizontalmente) ao processo do mesmo nível em outra estação, mas "descem" verticalmente através de cada nível adjacente da máquina transmissora até o nível físico (onde na realidade há a única comunicação horizontal entre máquinas), para depois "subir" verticalmente através de cada nível adjacente da máquina receptora até o nível de destino.

A arquitetura da rede é formada por níveis, interfaces e protocolos.

6.2 - NÍVEL FÍSICO (OU CAMADAS)

Fornece as características mecânicas, elétricas, funcionais e de procedimento, para ativar, manter e desativar conexões físicas para a transmissão de bits, entre entidades de nível de ligação, possivelmente através de sistemas intermediários.

Uma unidade de dados do nível físico consiste de um bit, em uma transmissão serial, ou "n" bits em uma transmissão paralela.

Ao projetista deste protocolo cabe decidir como representar 0's e 1's, quantos microssegundos durarão um bit, se a transmissão será "half-duplex" ou "full-duplex", com a conexão será estabelecida e desfeita, quantos pinos terá o conector da rede e quais seus significados, bem como outros detalhes elétricos e mecânicos.

A função do nível físico é a de permitir o envio de uma cadeia de bits pela rede sem se preocupar com o significado destes bits ou como são agrupados.

6.3 – NÍVEL DE LIGAÇÃO

O objetivo deste nível é detectar e opcionalmente corrigir erros que por ventura ocorram no nível físico. O nível de ligação vai assim converter um canal de transmissão não confiável, em um canal confiável para o uso do nível de rede. Em geral, todos os protocolos de nível de ligação incluem bits de redundância em seus quadros para detecção de erros, mas não a sua correção.

Quatro métodos são utilizados na delimitação dos quadros: contagem de caractere, transparência de caractere, transparência de bits e detecção de quadros pela presença ou ausência de sinal no meio físico.

6.4 - NÍVEL DE REDE

O objetivo deste nível é fornecer ao nível de transporte uma independência quanto às considerações de chaveamento e roteamento, associados com o estabelecimento e operação de conexão de uma rede.

6.5 - NÍVEL DE TRANSPORTE

O nível de rede necessariamente não garante que a cadeia de bits chegue ao seu destino. Pacotes podem ser perdidos ou mesmo reordenados. De forma a fornecer uma comunicação fim a fim verdadeiramente confiável é necessário outro nível de protocolo, que é justamente o nível de transporte. Este nível vai assim isolar dos níveis superiores à parte de transmissão da rede.

As principais funções deste nível de protocolo é o gerenciamento do estabelecimento e a desativação de uma conexão, o controle de fluxo e a multiplicação das conexões.

Além das funções mencionadas, podemos ainda citar como funções deste nível, o controle de sequência fim a fim, a detecção e recuperação de erros fim a fim, a segmentação e blocagem de mensagens, entre outras.

6.6 – EXERCÍCIO PROPOSTO

1) Quais são os níveis da Arquitetura de Rede?

_____
_____
_____

7 - MEIO DE TRANSMISSÃO

Neste capítulo iremos estudar sobre os meios de transmissão de dados pelos tipos de conexões físicas entre os computadores interligados na rede, tendo como exemplos, o cabo par trançado, o cabo coaxial e o cabo de fibra ótica.

7.1 – INTRODUÇÃO

Meio de transmissão é a conexão física entre as estações da rede. Geralmente, eles diferem com relação à faixa passante, potencial para conexão ponto a ponto ou multiponto, limitação geográfica devido à atenuação característica do meio, imunidade a ruído, custo, disponibilidade de componentes e confiabilidade.

A escolha do meio de transmissão adequado às aplicações é extremamente importante não só pelos motivos mencionados acima, mas também pelo fato de que ele influencia diretamente no custo das interfaces com a rede.

Qualquer meio físico capaz de transportar informações eletromagnéticas é possível de ser usado em redes locais. Os mais comumente utilizados são o par trançado, o cabo coaxial e a fibra ótica.

7.2 – PAR TRANÇADO

No par trançado, dois fios são enrolados em espiral de forma a reduzir o ruído e manter constantes as propriedades elétricas do meio através de todo o seu comprimento. A transmissão no par trançado pode ser tanto analógica, quanto digital. Radiação pode ocorrer quando a relação entre a separação dos condutores e a frequência de operação chega a um certo ponto. Como consequência, existe um limite na frequência de transmissão. A faixa passante do par trançado é notavelmente alta, considerando o fato de ele ter sido projetado para o tráfego analógico telefônico. Taxas de transmissão podem chegar até a ordem de alguns poucos megabits por segundo, dependendo da distância técnica de transmissão de condição e qualidade do cabo.

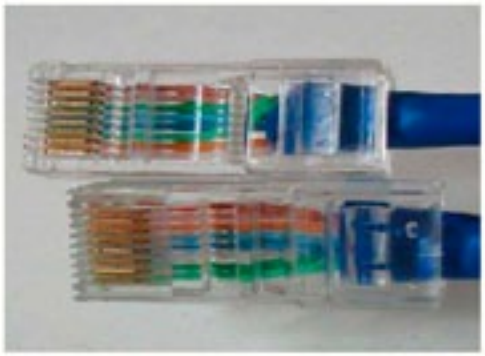

Figura 23 - Cabo Par Trançado.

7.3 – CABO COAXIAL

O cabo coaxial é uma forma de linha de transmissão que possui um condutor interno circundado por um condutor externo, tendo entre os condutores, um dielétrico, que os separa. O condutor externo é por sua vez circundado por outra camada isolante.

Existe uma grande variedade de cabos coaxiais, cada um com características específicas. Alguns são melhores para transmissão em alta frequência, outros têm atenuações mais baixas, outros são mais imunes a ruídos e interferências, etc. Os cabos de mais alta

qualidade não são maleáveis e são difíceis de instalar, mas cabos de baixa qualidade podem ser inadequados para altas velocidades e longas distâncias. O cabo coaxial, ao contrário do par trançado, mantém uma capacitância constante e baixa independente (teoricamente) do comprimento do cabo, evitando assim vários problemas técnicos. Devido a isto, oferecerá velocidades da ordem de megabits por segundo, sem ser necessária regeneração de sinal e sem distorções ou ecos, propriedade que revela a alta tecnologia já dominada. Os cabos coaxiais podem ser usados em ligações ponto a ponto ou multiponto. Ligações no cabo coaxial causam reflexão devido à impedância não infinita do conector ("transceiver"). A colocação destes conectores em ligações multiponto deve ser controlada de forma a garantir que as reflexões não se somem em fase a um valor significativo. Em uma rede em barra, o cabo deve ser casado em seus extremos (como da mesma forma o par trançado) de forma a impedir reflexões.

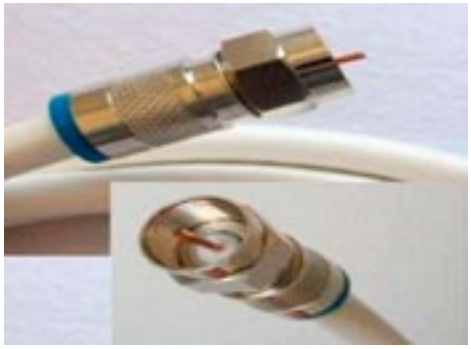

Figura 24 - Cabo Coaxial.

7.4 – FIBRAS ÓTICAS

A transmissão em fibra ótica é realizada pelo envio de um sinal de luz codificado, dentro do domínio de frequência do infravermelho, 1014 a 1015 Hz, através de um cabo ótico. O cabo consiste de um filamento de sílica ou plástico, por onde é feita a transmissão da luz. Ao redor do filamento existe outra substância de baixo índice de refração, que faz com que os raios sejam refletidos internamente, minimizando assim as perdas de transmissão. A fibra ótica é imune à interferência eletromagnética e a ruídos, e por não irradiar luz para fora do cabo, não se verifica "cross-talk". Ela permitirá uma isolação completa entre o transmissor e o receptor, fazendo com que o período de curto elétrico entre condutores não exista. A fibra ótica apresenta uma atenuação independente da frequência, permitindo assim uma velocidade de transmissão bastante alta (virtualmente ilimitada). Sob condições experimentais em laboratório, já foram obtidas taxas da ordem de alguns gigabits por segundo.

Figura 25 - Cabo de Fibra Ótica.

7.5 – EXERCÍCIOS PROPOSTOS

1) O que é Meio de Transmissão?

_____
_____
_____

2) Descreva Par Trançado, Cabo Coaxial e Fibra Ótica.

_____
_____
_____

8 - INTERLIGANDO SEGMENTO DE REDE LOCAL

Neste capítulo iremos falar sobre as distâncias que os sinais podem ser transportados de um ponto ao outro pela rede, e também vamos conhecer mecanismos utilizados para corrigir as perdas dos sinais numa distância muito longa, tais como, repetidores, pontes e Gateway.

8.1 – INTRODUÇÃO

Os sinais são transportados por distâncias limitadas antes de perderem energia. De um modo geral, em uma rede Ethernet, um sinal pode ser transportado em uma distância de até 300 metros; em um sistema Token Ring, em até 180 metros. As redes utilizam repetidores, pontes roteadores e Gateways para gerar e retransmitir sinais transportados em longas distâncias e para estabelecer comunicações com outras redes locais e remotas.

8.2 – REPETIDORES

Os repetidores fazem o que o próprio nome sugere: repetem sinais elétricos entre seções de cabos da rede. Os repetidores retransmitem sinais em ambas as direções indiscriminadamente. Dispositivos mais modernos, como pontes e roteadores, analisam as mensagens transportadas pelos sinais para determinar se é realmente necessário transmitir cada mensagem para o próximo segmento.

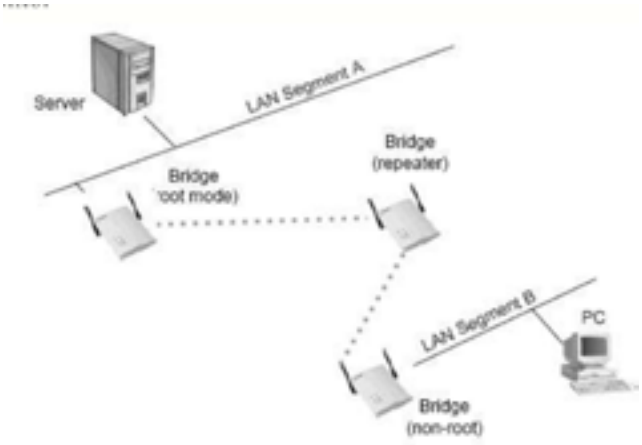

Figura 26 - Repedidores Wireless.

8.3 – PONTES

As pontes permitem combinar duas redes locais, além de admitir que estações de uma rede local acessem recursos de outra rede local. As pontes utilizam protocolos de controle de acesso ao meio físico (MAC) na física da rede. Através desse recurso, é possível ligar meios físicos diferentes entre si, como os cabos de fibra ótica e os cabos coaxiais 802.3, desde que as duas partes utilizem o mesmo protocolo de camada MAC (como Ethernet).

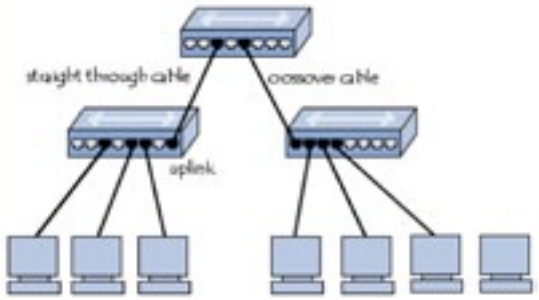

Figura 27 - Pontes de Redes.

8.4 – GATEWAY

Os Gateways, que são executados na camada de sessão do modelo OSI, permitem a comunicação entre redes que executam protocolos completamente incompatíveis entre si. Em geral, redes baseadas em PC's, os Gateways ligam os PC's a equipamentos host, como mainframes IBM.

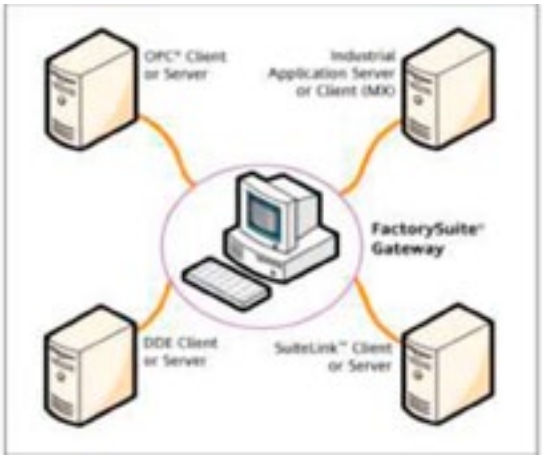
OPC™ Client or Server
Industrial Application Server or Client (MX)
FactorySuite® Gateway
DDE Client or Server
SuiteLink™ Client or Server

Figura 28 - Gateway.

8.5 – EXERCÍCIOS PROPOSTOS

1) Para que servem os Repetidores?

_____
_____
_____

2) O que são Pontes e Gateways?

_____
_____
_____

9 - ARQUITETURA TCP/IP

Neste capítulo iremos falar sobre o modelo da arquitetura TCP/IP, por que esse modelo foi criado, a finalidade dele nos dias de hoje, analisando sua importância no grande aparecimento da rede mundial de computadores, a internet, também iremos ver seu funcionamento e os serviços que essa arquitetura oferece.

9.1 - INTRODUÇÃO

As redes de computadores estão presentes no dia a dia das pessoas. Ao acessar uma conta de e-mail, ao manipular sua conta do banco online, ou até mesmo ao usar o celular, estamos acessando alguma informação armazenada em computadores interligados por uma rede, seja por fios ou não. Essa interatividade entre diferentes sistemas e plataformas de hardware e software tem como ferramenta principal o conjunto de serviços disponibilizados pela arquitetura TCP/IP. Compreender essa arquitetura e seus princípios fundamentais torna-se premissa básica para quem trabalha ou pretende trabalhar com redes de computadores e tecnologia da informação. Hoje, a arquitetura TCP/IP é padrão mundial na comunicação de dados em sistemas abertos, sendo a base do funcionamento da Internet.

O TCP/IP é um padrão internacional para comunicação entre sistemas operacionais, aplicações e plataformas diferentes. Essa arquitetura funciona como um conjunto de padrões e protocolos de comunicação de dados, utilizado na interconexão e endereçamento de computadores e redes.

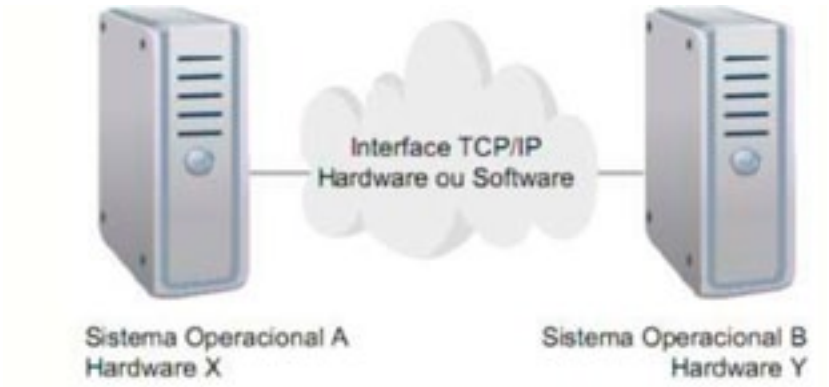

Figura 29 - Arquitetura TCP/IP em máquinas diferentes.

Cada computador deve possuir um programa de comunicação TCP/IP em seu sistema operacional e aplicativos, para se comunicar com outros dispositivos ou outras redes TCP/IP.
Os programas que controlam a comunicação de dados entre os equipamentos e aplicativos são chamados de protocolos de comunicação de dados. Os principais protocolos da arquitetura de rede são: TCP e o IP.

- **TCP:** é o protocolo responsável pelo controle e qualidade da comunicação entre a origem (transmissor) e o destino final (receptor).
- **IP:** é responsável pelo endereçamento das redes, de forma que os dados cheguem ao seu destino de acordo com o endereço de rede fornecido.

9.2 - CAMADAS DA ARQUITETURA

A arquitetura TCP/IP divide o processo de comunicação em quatro camadas. Em cada camada atuam determinados protocolos que interagem com os protocolos das outras camadas da arquitetura TCP/IP.

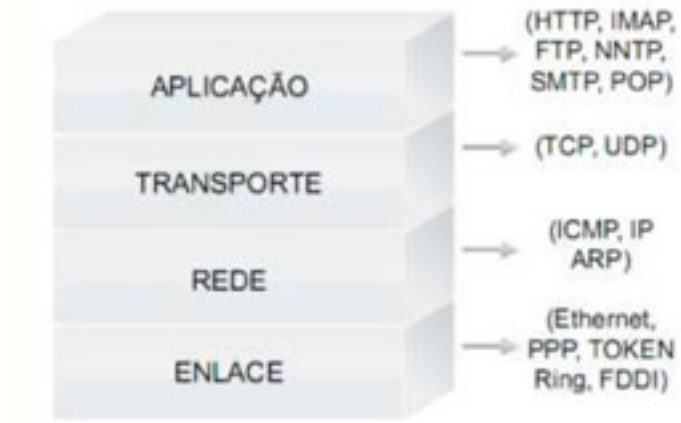

Figura 30 - Camadas TCP/IP e Protocolos.

- **Camada de Aplicação -** protocolos de aplicações: FTP, TEL-NET, DNS, SNMP, SMTP, entre outros.
- **Camada de Transporte -** protocolos de transporte: TCP, UDP.
- **Camada de Rede -** protocolos de endereçamento de rede: IP, ARP, RARP, ICMP.
- **Camada de Enlace -** (acesso à rede, interface de rede ou Data-Link): protocolos de acesso ou enlace físico: CSMA/CD-Ethernet, PPP, HDCL, Token-ring, FDDI, que interagem com o hardware e o meio de transmissão, permitindo que as camadas de cima independam do meio de transmissão utilizado.
- **Camada Física -** no modelo TCP/IP, a camada física está englobada na camada de enlace, diferentemente do modelo OSI, onde a camada física é representada individualmente. A camada física é composta pelo hardware, sinais elétricos, meios de transmissão e seus padrões.

A divisão do processo de comunicação de dados em camadas tem como objetivo modular, ou seja, dividir o processo de comunicação em etapas menores e específicas para facilitar o controle e o desenvolvimento de produtos e sistemas de comunicação de dados.

9.2.1 – CAMADAS DE APLICAÇÕES

Nesta camada ficam os protocolos responsáveis pela comunicação com as diferentes aplicações. Podem-se separar os protocolos de aplicação em protocolos de serviços básicos e de serviços para o usuário. Protocolos de serviços básicos, que fornecem serviços para atender as próprias necessidades do sistema de comunicação TCP/IP:

- **DNS (Domain Name System):** esse protocolo é uma aplicação que associa o nome simbólico WWW de um site ao seu endereço IP, de forma a encaminhar os dados para ele. Essa aplicação é processada em servidores. Quando digitamos um site que desejamos acessar, como por exemplo: www.xyz.com.br, ela descobre por meio de tabelas o endereço IP dele e os dados são encaminhados para esse endereço.
- **BOOTP (Bootstrap Protocol):** é um protocolo que permite a configuração automática de parâmetros de rede, porém sem a capacidade de alocar dinamicamente esses parâmetros, como faz o DHCP. Esse protocolo tornou-se limitado pelas exigências atuais.
- **DHCP (Dynamic Host Configuration Protocol):** é um protocolo que oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.

9.2.1.1 - PROTOCOLO DE SERVIÇO PARA USUÁRIO

- **Telnet (Terminal Emulation):** protocolo utilizado para acessar outros computadores e simular/emular um terminal para acessar informações

remotamente.

- **FTP (File Transfer Protocol):** protocolo utilizado para fazer a transferência de arquivos, criação e alteração de diretórios. A transferência de arquivos pode ocorrer de dois modos: texto ou binário.

9.2.2 – CAMADAS DE TRANSPORTE

A camada de transporte tem como função estabelecer uma conexão fim a fim (também chamada de conexão confiável) entre a origem e o destino dos dados, garantindo a integridade dos dados na transmissão, checando se não ocorreram perdas de pacotes e se eles estão chegando na sequência correta. Ela solicita a retransmissão de pacotes faltantes ou com erro e efetua um controle de luxo do envio dos dados entre a aplicação e a transmissão dos dados pela rede. Esta camada possui dois protocolos que são o UDP (User Datagram Protocol) e o TCP (Transmission Control Protocol). O primeiro realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente. O segundo, além da multiplexação, realiza uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP: o controle de luxo, o controle de erro, a sequenciação e a multiplexação das mensagens.

Multiplexação é a técnica que permite a transmissão de mais de um sinal em um mesmo meio físico.

Lembrando que o protocolo UDP é menos confiável que o TCP, pois este realiza também o controle de luxo e os erros nas mensagens.

9.2.3 – CAMADAS DE REDE

Nessa camada são definidos e tratados os endereços lógicos de origem e de destino na rede, os caminhos que os dados irão percorrer para atingir o seu destino e a interconexão de múltiplos links. O endereçamento utilizado pelo protocolo IP é estruturado em 32 bits, e foi desenvolvido para facilitar interligação dos dispositivos. Este endereçamento é composto por quatro inteiros separados por pontos. Essa representação é conhecida como notação em pontos decimais. Segue abaixo uma tabela com 5 classes de endereço IP.

CLASSE	FAIXA DE ENDEREÇOS
Classe A	0.1.0.0 – 126.0.0.0
Classe B	128.0.0.0 – 191.255.0.0
Classe C	192.0.1.0 – 223.255.255.0
Classe D	224.0.0.0 – 239.255.255.255
Classe E	240.0.0.0 – 247.255.255.255

9.2.4 – CAMADAS DE ENLACE DE REDE

A camada de interface de rede é a camada de mais baixo nível dentro do modelo. Ela é responsável por colocar e retirar quadros (frames, pacotes) no meio físico. Nesta camada estão os protocolos utilizados nas diversas tecnologias de comunicação física de rede. Esses protocolos não fazem realmente parte da suíte TCP/IP, mas sim permitem que um host TCP/IP se comunique com outros hosts na rede. Podemos ter protocolos de enlace para redes locais (LAN's) e outros utilizados para redes de longa distância (WAN's). Nas LAN's, os protocolos de acesso ao meio, são Ethernet-CSMA/CD, Token-ring e FDDI. O primeiro tem as suas especificações descritas no padrão IEEE (Instituto de Engenheiros Eletricistas e Eletrônicos) 802.3. A camada de Enlace, nas redes Ethernet, possui duas subcamadas como no modelo OSI, que será visto mais à frente.

- **MAC (Media Access Control):** IEEE 802.3, que define como transmitir frames no meio físico, manipulando o endereço físico associado a cada dispositivo, controle de fluxo opcional e notificação de erro.
- **LLC (Logical Link Control):** IEEE 802.2, que identifica diferentes tipos de protocolos da camada superior e os encapsula.

MAC address ou **endereço MAC** é um identificador único, associado pelo fabricante, aos adaptadores de rede ou placas de interface de rede para sua própria identificação.

9.3 – EXERCÍCIO PROPOSTO

1) Quais são os principais protocolos da arquitetura de rede? Cite suas definições.

_____
_____
_____

10 - PROTOCOLO TCP/IP

No capítulo anterior vimos uma breve explanação da arquitetura TCP/IP, seus modelos de protocolos e a sua utilização em cada camada do modelo. Neste capítulo iremos falar sobre os detalhes, sobre os protocolos necessários para comunicação de dados na rede, vendo a função de cada um.

10.1 – INTRODUÇÃO

Os protocolos de comunicação de dados são como as linguagens de comunicação. Duas pessoas para se comunicarem necessitam falar a mesma língua. Da mesma forma, dois computadores ou equipamentos para se comunicarem precisam utilizar o mesmo protocolo de comunicação. Os protocolos de comunicação de dados são simplesmente programas que ficam carregados na memória dos computadores e têm como função controlar a comunicação de dados entre dois pontos ou em uma rede. A maioria dos protocolos especifica uma ou mais das seguintes propriedades:

a) Detecção da conexão física subjacente ou a existência de um nó.
b) Estabelecimento de uma conexão.
c) Negociação de várias características de uma conexão.
d) Como inicializar e finalizar uma mensagem.
e) Como formatar uma mensagem.
f) O que fazer com mensagens corrompidas ou mal formatadas.
g) Como detectar perdas inesperadas de conexão e o que fazer em seguida.
h) Término de sessão ou conexão.

O uso difundido e a expansão dos protocolos de comunicação formaram um pré-requisito e uma contribuição para o poder e sucesso da Internet. O par formado pelo TCP e IP é uma referência a uma coleção dos protocolos mais utilizados. A maioria dos protocolos para comunicação via Internet é descrita nos documentos RFC da IETF.

RFC é um acrônimo de Request for Comments. Ele é um documento que descreve os padrões de cada protocolo da Internet.

Os protocolos raramente trabalham sozinhos, pois geralmente são implementados como pilhas de protocolos, onde cada nível desta pilha se especializa em funções diferentes, facilitando assim a modularidade do sistema. Os protocolos de uma camada se comunicam com seu correspondente na mesma camada de destino, utilizando os protocolos e camadas de baixo para enviar seus dados.

10.2 – PROTOCOLO DA ARQUITERUTA TCP/IP

O TCP/IP não é um único protocolo ou programa de controle de comunicação, mas um conjunto de protocolos que controla a comunicação de dados em redes de computadores, o que já foi visto no capítulo anterior. Como vimos, a arquitetura é dividida em quatro camadas para um melhor entendimento e divisão das funções de cada componente que faz parte da comunicação de dados. São os protocolos mais comuns.

10.2.1 - PROTOCOLO HTTP (HYPERTEXT TRANSFER PROTOCOL)

Este é um protocolo que faz a comunicação entre o browser (programa cliente responsável pelo recebimento de páginas web) do computador e o servidor web.

A Figura 31 mostra um exemplo de browser utilizado por muitas pessoas, o Google Chrome. Neste caso, ele recebeu um documento virtual da Internet, referente ao site do Yahoo, e o interpretou como um documento com figuras, textos, formulários e links.

Figura 31 - Browser interpretando uma página HTML.

Usualmente, este protocolo utiliza a porta 80 e é usada para a comunicação de sites (sítios) web, utilizando o HTML. Esta linguagem de computador permite a criação de hiperlinks (âncoras) nas páginas web, fornecendo acesso a outros documentos.

Hypertext Markup Language (HTML), que significa Linguagem de Marcação de Hipertexto, é uma linguagem de marcação utilizada para construir páginas na web. Essas páginas podem ser interpretadas pelos browsers (navegadores).

10.2.2 - PROTOCOLO TELNET (TERMINAL EMULADOR)

É uma aplicação que faz a conexão e a simulação de um host que acessa um servidor ou equipamento, para acessar seus dados como se esse host fosse uma estação local do servidor. Em outras palavras, TELNET é um protocolo de login remoto.

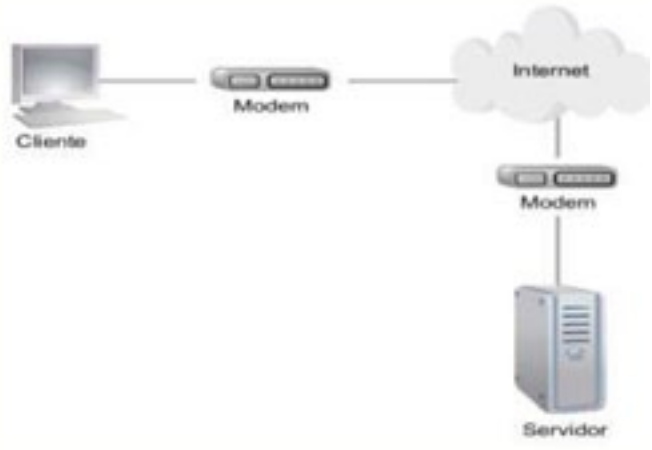

Figura 32 - Protocolo TELNET.

Temos um computador acessando um servidor remoto através da Internet. O acesso a outro computador remoto, usando esse protocolo, pode ser feito por cabo conectado diretamente, ou via uma rede como a Internet para acessar um sistema remoto (servidor, estações, ou outra rede), como mostrado na Figura 32.

10.2.3 - PROTOCOLO FTP (FILE TRANSFER PTOTOCOL)

É uma aplicação da arquitetura TCP/IP utilizada para transferência de arquivos entre dois computadores. O FTP permite interatividade entre o cliente (computador que solicita o arquivo) e o servidor (computador que irá fornecer o arquivo), com segurança por meio de logins e senhas.

10.2.4 - PROTOCOLO SMTP (SIMPLE MAIL TRANSFER PTOTOCOL) E POP

(POST OFFICE PROTOCOL)

Analogamente ao protocolo HTTP, os protocolos SMTP e POP são responsáveis pela comunicação entre um computador e um servidor, neste caso um servidor de correio eletrônico para recebimento e envio de mensagens de e-mail respectivamente. O SMTP é um protocolo relativamente simples, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados e, na maioria dos casos, validados, sendo depois a mensagem transferida. O SMTP é apenas um protocolo de envio, o que significa que ele não permite que um usuário descarregue as mensagens de um servidor. Para isso, é necessário um cliente de e-mail com suporte ao protocolo POP ou IMAP, que é o caso da maioria dos clientes atuais.

O protocolo IMAP (Internet Message Access Protocol) possui mais recursos que o protocolo POP3 e permite ao internauta ter acesso a suas pastas e arquivos em qualquer computador, tanto por webmail, como por cliente de correio eletrônico (ex.: Outlook Express, Evolution).

10.2.5 - PROTOCOLO SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

É um protocolo de comunicação usado para transmitir informações de status de equipamentos conectados em rede a um servidor gerenciador dessas informações. Assim são feitas estatísticas e análises da rede, como a avaliação do tráfego, visando obter subsídios para efetuar ações corretivas ou de expansão e adequação da rede, por exemplo.

10.2.6 - PROTOCOLO IP

O IP é um protocolo usado entre duas ou mais máquinas em rede para encaminhamento dos dados. Os dados numa rede IP são enviados em blocos referidos como pacotes ou datagramas.

Características básicas do protocolo IP:

- A entrega do pacote IP não é garantida pelo protocolo, ou seja, podem ocorrer perdas de pacote ao longo da transmissão.
- É um protocolo não orientado à conexão.
- Os pacotes podem se perder, atrasar ou serem entregues fora de ordem.
- Cada pacote pode seguir diferentes rotas (caminhos).
- Os pacotes IP têm um tempo de vida para trafegar na rede, após o qual, não alcançando seu destino, são descartados pela rede para não ficar vagando e ocupando seus recursos.

Fica a dica

O IPv6 é a versão mais atual do protocolo IP. Ele está sendo implantado gradativamente e deve funcionar lado a lado com o IPv4, por algum tempo, numa situação tecnicamente chamada de pilha dupla ou dual stack. Enquanto o IPv4 suporta cerca de 4 bilhões de endereços, o novo protocolo IPv6 suporte cerca de 3.4 x endereços.

10.2.7 - PROTOCOLO ICMP

O protocolo ICMP (Internet Control Message Protocol) é utilizado para fornecer relatórios de erros à fonte original. Qualquer computador que utilize IP precisa aceitar as mensagens ICMP e alterar seu comportamento de acordo com o erro relatado. O protocolo ICMP costuma enviar mensagens automaticamente quando um determinado pacote não consegue chegar ao seu destino final, ou quando o Gateway está congestionado.

Gateways são máquinas intermediárias, geralmente destinadas a interligar redes, separar domínios, ou mesmo traduzir protocolos (ex.: roteadores e firewalls).

10.3 – EXERCÍCIO PROPOSTO

1) Quais são as propriedades que a maioria dos protocolos especifica?

_____
_____
_____

11 - ENDEREÇAMENTO IP

11.1 – INTRODUÇÃO

No capítulo anterior vimos os principais protocolos da arquitetura TCP/IP e suas principais funcionalidades. Neste capítulo iremos falar como funciona a transmissão de dados de uma máquina para outra na rede, utilizando o modelo TCP/IP.

11.2 – CONCEITOS

Endereços IP no formato X.X.X.X – conhecidos pelo termo inglês dotted quad – são a expressão, em números decimais, de um número de rede binário. Cada um dos quatro campos separados por pontos corresponde a um byte, algumas vezes chamamos octeto. Por exemplo, o número IP 192.168.1.1 corresponde à forma binária: 11000000. 10101000.00000001.00000001.

Tabela de Conversão de Binário para Decimal.

Binário	Exponenciação	Decimal
00000001	2^0	1
00000010	2^1	2
00000100	2^2	4
00001000	2^3	8
00010000	2^4	16
00100000	2^5	32
01000000	2^6	64
10000000	2^7	128

11.3 – CLASSE DE ENDEREÇO

Cada interface em uma mesma rede deverá ter um endereço IP único, mas cada computador pode possuir mais de uma interface de rede. Mesmo que exista apenas uma interface, é possível criar interfaces virtuais sobre ela, como é o caso de uma rede VPN. Dessa forma, o computador se comunica como se houvessem duas interfaces, cada uma conectada a uma rede distinta.

Inicialmente, o espaço do endereço IP foi dividido em algumas estruturas de tamanho fixo chamadas de "classes de endereço". As três principais são a Classe A, Classe B e Classe C. Examinando os primeiros bits de um endereço, o sistema operacional é capaz de determinar qual a classe do endereço. A estrutura das classes é:

- **Classe A:** primeiro bit é 0.
- **Classe B:** primeiros dois bits são 10.
- **Classe C:** primeiros três bits são 110.
- **Classe D:** (endereço multicast): primeiros quatro bits são 1110.
- **Classe E:** (endereço especial reservado): primeiros quatros bits são 1111.

Classe	Faixa de Endereço	Número de IPs Possíveis
A	1.0.0.0 até 126.0.0.0	16.777.216
B	128.0.0.0 até 191.255.0.0	65.536
C	192.0.0.0 até 223.255.255.254	256
D	224.0.0.0 até 239.255.255.255	Multicast
E	240.0.0.0 até 255.255.255.255	Multicast Reservado

11.4 – CLASSES ESPECIAIS

Classes especiais ou classes reservadas são utilizadas, por exemplo, para a comunicação com uma rede privada ou dentro do próprio computador local. A faixa IP que trafega entre 127.0.0.0 e 127.255.255.255 é reservada para a comunicação com o computador local (local host). Qualquer pacote enviado para estes endereços permanece no computador que os gerou. Essa abordagem permite à aplicação comunicar-se com os serviços presentes na própria máquina local.

11.5 – ENDEREÇO DE REDE

Para que os dados possam ser encaminhados corretamente pela rede, a interface de rede precisa conhecer seu número IP, o número IP de destino e a qual rede eles pertencem. Na maioria dos casos, a rede do IP de destino só será conhecida quando esse IP de destino estiver dentro da mesma rede interna do IP de origem. É possível identificar se um IP pertence a uma rede fazendo o cálculo a partir da máscara de rede.

O cálculo é feito a partir da forma binária dos números IP.

- Máscara de 16 bits: 11111111.11111111.00000000.00000000 = 255.255.0.0.
- Máscara de 17 bits: 11111111.11111111.10000000.00000000 = 255.255.128.0.

Na primeira máscara (16 bits), pertencerão à mesma rede os IP's cujos dois primeiros octetos do endereço não difiram entre si. Na segunda máscara (17 bits), pertencerão à mesma rede os IP's cujos dois primeiros octetos e o primeiro bit do terceiro octeto do endereço não difiram entre si. Dessa forma, dois endereços de interface 172.16.33.8 e 172.16.170.3 estarão na mesma rede se a máscara for de 16 bits, mas não se a máscara for de 17 bits.

As máscaras de rede variam dependendo do contexto da rede. Consequentemente, o endereço da rede corresponde à parte do número IP determinado pelos bits marcados da máscara de rede. Para uma máquina 172.16.33.8 com máscara de rede 255.255.0.0, o endereço da rede será 172.16.0.0.

11.6 – DHCP

Como pudemos perceber nas seções anteriores, a administração de endereços IP é trabalhosa. Para automatizar parte dessa tarefa, foi criado o protocolo DHCP (Dynamic Host Configuration Protocol), o qual, por meio de um servidor DHCP, distribui automaticamente endereços, máscaras, Gateway padrão e outras configurações para os hosts da rede. Além do servidor DHCP, os computadores da rede devem possuir um software DHCP para se comunicar com esse servidor. Esse software DHCP solicita e obtém do servidor DHCP

as configurações básicas do TCP/IP, como: endereço IP, máscara e default Gateway (ou roteador padrão), quando é ligado.

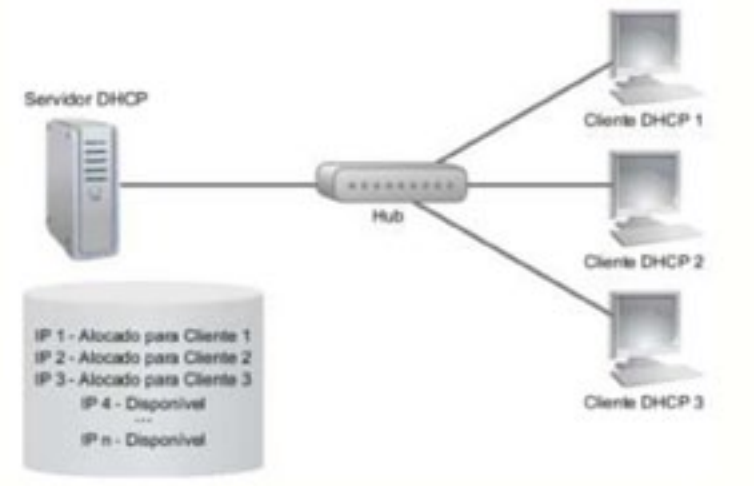
Servidor DHCP
Hub
Cliente DHCP 1
Cliente DHCP 2
Cliente DHCP 3
IP 1 - Alocado para Cliente 1
IP 2 - Alocado para Cliente 2
IP 3 - Alocado para Cliente 3
IP 4 - Disponível
IP n - Disponível

Figura 33 - Servidor DHCP.

O exemplo da Figura 33 mostra uma rede utilizando o protocolo DHCP. Note que no servidor DHCP é mantida uma base de dados com os números IP's que já foram alocados a algum computador Cliente, e os valores que ainda estão disponíveis para locação. Percebe-se que a configuração de faixa de IP, máscara de rede, e outras informações de configuração da rede ficam armazenadas no servidor, facilitando a administração de endereços.

11.7 – EXERCÍCIO PROPOSTO

1) Descreva a estrutura de classe do endereço IP.

_____
_____
_____

12 – ROTEADORES

12.1 – INTRODUÇÃO

Neste capítulo vamos ver os conceitos de roteadores e o roteamento dos dados em uma rede TCP/IP, ou seja, os vários caminhos possíveis de enviar informações de uma máquina de origem a uma máquina de destino.

12.2 – CONCEITOS

Roteadores são equipamentos que encaminham os dados através de uma ou mais redes, utilizando o endereço IP do pacote de dados que está sendo transmitido. Assim, os roteadores são utilizados para interconectar redes diferentes ou distantes entre si. Os roteadores utilizam tabelas de rotas para decidir sobre o encaminhamento de cada pacote de dados recebido. Eles preenchem e fazem a manutenção dessas tabelas executando processos e protocolos de atualização de rotas, especificando os endereços e domínios de roteamento, atribuindo e controlando métricas de roteamento. O administrador de rede pode fazer a configuração estática das rotas para a propagação dos pacotes, ou pode configurar o roteador para que este atualize sua tabela de rotas através de processos dinâmicos e automáticos.

Figura 34 - Roteador Wireless.

Temos na Figura 34 um roteador wireless (sem fio) da marca D-Link, que possui 1 porta Internet e 4 portas Ethernet 10/100. Interessante notar que os roteadores atuais de mercado fazem mais que apenas rotear pacotes de dados na rede. Para tratar os dados das tabelas de roteamento e escolher o melhor caminho ou rota para que os dados cheguem ao seu destino, os roteadores utilizam protocolos de roteamento que executam essas funções. Os protocolos de roteamento mais conhecidos são o RIP e o OSPF.

12.3 – PROTOCOLO DE ROTEAMENTO

Chamamos de protocolo de roteamento aqueles que controlam e fazem o encaminhamento dos dados entre os roteadores, o controle e a atualização das tabelas de roteamento, a escolha da melhor rota para os dados chegarem ao destino e demais funções relativas às operações de roteamento. Exemplos: RIP (Routing Information Protocol) e o OSPF (Open Shortest Path First).

Chamamos de protocolos roteáveis aqueles que transmitem pacotes de dados com endereços de rede que podem ser lidos, tratados e encaminhados nos roteadores pelos protocolos de roteamento. Exemplos: IP e o IPX (utilizado na arquitetura NetWare).

Netware é um sistema operacional para servidores de arquivos, desenvolvido pela Novell.

12.4 – ROTEAMENTO ESTÁTICO E DINÂMICO

Roteadores atuais implementam roteamento dinâmico, tornando mais simples as tarefas de configuração. No entanto, o roteamento estático é muito importante e inúmeras aplicações exigem o seu uso.

Nos roteadores estáticos, as tabelas de roteamento são criadas e configuradas de forma manual. Quando um endereço é alterado ou as rotas deslocadas, será necessária uma intervenção manual para a atualização da tabela de roteamento.

Roteadores dinâmicos trocam rotas periodicamente, aprendendo novos caminhos. A responsabilidade pela atualização das rotas é dos algoritmos de inter-roteamento.

13 - FUNDAMENTOS DE REDES WAN'S

13.1 – INTRODUÇÃO

Neste capítulo iremos falar dos conceitos iniciais, compreender os conceitos de estrutura e o funcionamento da rede Wan.

13.2 – CONCEITOS

Uma rede WAN (Wide Area Network) geralmente abrange várias cidades, vários países e até mesmo continentes. Uma característica muito importante neste tipo de rede é que ela é escalável, ou seja, tem capacidade de aguentar mais serviços e de crescer em nível de dispositivos e enlaces.

Por exemplo, pense em uma grande empresa multinacional com escritórios espalhados por vários países. Uma rede WAN deve ser capaz de se comunicar com todos os computadores e grandes servidores desta empresa, permitindo a conexão entre estes dispositivos com desempenho razoável.

Percebemos que para construir uma rede nestas proporções requer maiores recursos tecnológicos, algoritmos de roteamento mais eficientes e equipes de suporte mais especializadas. Uma das tecnologias de transporte de dados utilizadas neste tipo de rede é o MPLS, que permite a transmissão de informações com o menor número de erros.

MPLS (Multi Protocol Label Switching) é um mecanismo de transporte de dados pertencente à família das redes de comutação de pacotes.

> *A implementação de uma WAN cada vez mais demanda um bom planejamento por parte das empresas e administradores de redes. A forma de acesso à Internet (maior rede WAN existente) que mais vem crescendo recentemente é o acesso através da banda larga. Segundo pesquisa realizada no ano de 2006, pela IDC Brasil, o crescimento foi de 40,1%. Tal percentual representa 1,6 milhão de novas conexões, o que totaliza 5,7 milhões de usuários no território nacional. Em resumo, no período de seis anos (2001 a 2006), a banda larga cresceu 1.639% no Brasil. Tal fatia do mercado simboliza, no entanto, apenas 3% da população brasileira, sendo que 60,7% dos acessos são efetuados na região Sudeste, cabendo ao estado de São Paulo 39% desse total. A tecnologia mais utilizada no acesso à banda larga é o xDSL, que equivale a 78,2% das conexões banda larga existentes no país. O avanço de novas tecnologias no mercado ainda possibilitou ao consumidor brasileiro uma diminuição do valor de acesso banda larga. A concorrência, em especial entre as operadoras de TV a cabo e as de telefonia, pela preferência do consumidor, resultou em uma queda de preço de aproximadamente 8%. Tal diminuição ainda possibilitou a alteração da velocidade já utilizada pelos assinantes. Preços menores foram os principais responsáveis pela opção dos consumidores por bandas com maior velocidade. Os acessos superiores a 1 Mbps saltaram de 2% do mercado em dezembro de 2005 para 22% no mesmo período de 2006. As velocidades acima de 512 Kbps representaram 37% do mercado. (WIKIPEDIA-REDESWAN, 2009)*

xDSL é o nome genérico para os diversos padrões de tecnologia telefônica digital, que têm como características principais: uso simultâneo de telefone e transmissão de dados e alta taxa de transferências.

Porém, como uma rede WAN pode permitir o acréscimo de mais dispositivos sem reduzir bruscamente seu desempenho de transmissão de informações? Para tal, este tipo de configuração não possui a interligação ponto a ponto entre as máquinas, mas sim a interligação dos dispositivos de rede através de switches.

Switches, também denominados de Switch de Pacotes, são pequenos computadores (pois possuem processador, memória e dispositivos de E/S) que são capazes de transmitir pacotes completos de uma conexão para outra.

> *O tráfego das WAN's aumenta continuamente surgindo em função disso mais congestionamento do que será transportado na rede, definindo as características destes tráfegos (voz, dados, imagens e vídeo), qualidade de serviço (QoS), protocolos ultra compreensão. O tráfego da rede tem que ser modelado através de medições com um grau de resolução elevado, incluindo a análise de pacotes a fim de disponibilizar aos interessados usando técnicas gráficas, estatísticas descritivas, entre outros. Quando ocorre variação na chegada de pacotes, isso indica que a Wan está consistente e seu tráfego pode ser acelerado de acordo com as necessidades dos serviços. (WIKIPÉDIA-REDESWAN, 2009)*

Alguns protocolos de redes WAN que permitem a transmissão de dados em redes de longa distância:

- **PPP:** Protocolo Ponto a Ponto, comumente utilizado para conexão à Internet. Bem conhecido pelos fãs do sistema Unix.
- **Rede X.25:** Fornece uma arquitetura orientada à conexão, porém apresenta uma alta taxa de erros.
- **Frame Relay:** Sucessor do X.25, fornece vários tipos de serviços em altas velocidades.

Outro aspecto importante em redes WAN é a segurança da informação, já que temos vários sistemas interligados e diversos usuários com diferentes propósitos conectados através da Internet.

13.3 – EXERCÍCIOS PROPOSTOS

1) O que é uma rede WAN?

_____
_____
_____

2) Exemplifique alguns protocolos de rede WAN.

_____
_____
_____

14 - MODELO DE REFERÊNCIA OSI

Neste capítulo iremos falar sobre a padronização consagrada para o mundo das redes de computadores, chamada modelo OSI.

14.1 – INTRODUÇÃO

As primeiras redes de computadores surgiram com soluções proprietárias, isso quer dizer que qualquer equipamento ou software para aquela rede deveria ser adquirida com o mesmo fabricante, pois equipamentos e softwares de fabricantes diferentes não se comunicavam. Assim, um único fabricante era o responsável por fornecer todos os componentes de rede que você precisaria.

Para que fabricantes diferentes criassem a interconexão de sistemas de computadores, foi necessário estabelecer uma padronização para as redes. Então o modelo RM-OSI (Reference Model – Open System Interconnection – Modelo de Referência – Interconexão de Sistemas Abertos) surgiu. Esse modelo baseia-se em uma proposta desenvolvida pela ISO (International Standards Organization – Organização Internacional de Padronizações).

Figura 35 - Comunicação entre Protocolos.
Fonte: Criação feita pelos autores.

Esses dois protocolos são apenas exemplos de vários outros que são utilizados nas redes, cuja comunicação foi dividida em camadas.

14.2 – CAMADAS DO MODELO OSI

O modelo de referência OSI é um modelo teórico que os fabricantes devem seguir para que sistemas diferentes possam trocar informações. Foram adotadas sete camadas: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace de Dados e Física.

OSI - Organização Internacional para Padronização Foi fundada em 23 de fevereiro de 1947, aprova todas as normas internacionais nos campos técnicos, exceto eletricidade e eletrônica, que fica a cargo da IEC (International Eletrotechnical Commission).

Figura 36 - Camadas do Modelo OSI.
Fonte: http://gridra.files.wordpress.com/2008/09/osi2.jpg

> *As camadas são numeradas de 1 a 7 (de baixo para cima). Assim, muitas vezes nas aulas e nos livros, citamos apenas o número da camada: "a camada 3 fornece suporte ao protocolo IP". Fica subentendido que estamos falando da camada de rede, embora seja apenas um modelo teórico, que não precisa necessariamente ser seguido à risca pelos protocolos de rede. O modelo OSI é interessante, pois serve como deixa para explicar diversos aspectos teóricos do funcionamento da rede. (MORIMOTO, 2008)*

14.2.1 – CAMADA 7 – DE APLICAÇÃO

Nesta camada, o programa solicita os arquivos para o sistema operacional e não se preocupa como será feita a entrega desses arquivos, pois isso fica a cargo das camadas mais baixas. Por exemplo: quando você digita o endereço http://www.google.com, você apenas recebe o conteúdo da página (que é um arquivo), caso ela exista e esteja disponível.

IP: primeiro contato: é quase impossível falar de internet sem falar de IP. Cada site na internet é encontrado por endereçamento IP, que funciona como se fosse o número do telefone do seu computador. Você não consegue decorar os números IP de cada site; é mais fácil decorar o nome.

14.2.2 – CAMADA 6 – DE APRESENTAÇÃO

Como o próprio nome sugere, trata-se de se apresentar os dados de forma inteligível ao protocolo que vai recebê-lo. Podemos citar como exemplo, a conversão do padrão de caracteres (afinal, existem diversos alfabetos diferentes) de páginas de código.

14.2.3 – CAMADA 5 – DE SESSÃO

Permite que dois programas em computadores diferentes estabeleçam uma sessão de comunicação. O evento da sessão tem algumas regras, as aplicações definem como será feita a transmissão dos dados e colocam uma espécie de marca no momento da transmissão. Quando acontecer uma falha, apenas os dados depois da marcação serão transmitidos.

Você pode entender o conceito de Sessão como a duração de uma ligação telefônica: a ligação tem um processo para ser iniciada, há uma troca de mensagens durante o tempo da ligação e depois há um processo de término. Assim, quando você entra em um site, uma sessão é aberta para você naquele servidor; depois de navegar pelo site, você poderá encerrar essa seção, ou pode simplesmente sair para outro site; neste caso o servidor encerrará sua seção depois de ficar algum tempo sem uma resposta sua.

14.2.4 – CAMADA 4 – DE TRANSPORTE

Também é um nome bem sugestivo para a função. Esta camada é a responsável por transportar os dados provenientes da camada de sessão. Como qualquer transporte por caminhão, sua carga precisa estar devidamente empacotada e endereçada com remetente e destinatário. A camada de transporte inicialmente faz isso. Essa camada controla o fluxo (colocando os pacotes em ordem de recebimento), corrigindo os erros através do envio de uma mensagem chamada ACK (Acknowledge – Reconhecimento). Um protocolo muito conhecido desta camada é o TCP (Transmission Control Protocol – Protocolo de Controle de Transmissão).

O **ACK** é um pacote enviado ao transmissor para informa-lo de que os pacotes foram recebidos com sucesso. Em caso negativo, é enviado um NACK que, como o nome sugere, é uma negação do ACK, dizendo que o pacote não foi entregue corretamente ou não chegou.

14.2.5 – CAMADA 3 – DE REDE

Esta camada é uma das mais conhecidas, pois nela são tratados os endereços de rede, conhecidos resumidamente como IP (Internet Protocol). Os endereços IP são números pré-definidos, atribuídos aos computadores que compõem uma rede.

Mais sobre IP:

IP é um número de 32 bits que define o endereço de uma rede ou de um computador, escrito em quatro blocos separados por ponto. Exemplos: 192.168.10.33

14.2.6 – CAMADA 2 – DE ENLACE

Nesta camada, os pacotes que vêm da camada de rede com endereços IP já definidos são transformados em "quadros" ou "frames". Os quadros acrescentam outra forma de endereçamento chamada endereço MAC (Media Access Control – Controle de Acesso ao Meio).

MAC é um endereço exclusivo da placa de rede. Os fabricantes adotam um processo de numeração para garantir que não ocorram números MAC iguais em suas placas. Assim, é garantido que numa rede não existam dois endereços físicos iguais. O número contém 48 bits, normalmente escrito em notação hexadecimal, por exemplo: 00-C0-95-EC-b7-93.

14.2.7 – CAMADA 1 – DE FÍSICA

Os dados provenientes da camada de enlace com os endereços já pré-estabelecidos, são transformados em sinais que serão transmitidos pelos meios físicos. Assim, a camada física converte os quadros de bits 0 e 1:

- em sinais elétricos, caso o meio físico seja o cabo de cobre;
- em sinais luminosos, caso o meio físico seja a ibra óptica;
- em frequência de rádio, caso seja uma rede sem fio.

14.3 – EXERCÍCIO PROPOSTO

1) Quais são as camadas do modelo de referência OSI e suas finalidades?

_____
_____
_____

15 - MEIO FÍSICO DE TRANSMISSÃO I

Neste capítulo iremos nos concentrar mais na transmissão, compreendermos como os meios físicos são utilizados e quais são eles. Também veremos as características de cada um e como são utilizados.

15.1 – INTRODUÇÃO

> *Basicamente, a função de qualquer meio de transmissão é carregar um fluxo de informações através de uma rede, ficando essa capacidade de transmissão limitada apenas pelas características particulares de cada um. Os meios (ou mídias) de transmissão são divididos em dois grupos: meios guiados, como os fios de cobre e os cabos de fibras ópticas e os meios não guiados, como as ondas de rádio e os raios laser transmitidos pelo ar. (PINHEIRO, 2003)*

Nesse momento estudaremos os meios guiados: cabos de par trançado, cabos coaxiais e fibras ópticas. No próximo capítulo, estudaremos os meios não guiados, que usam o ar como meio físico de transmissão.

15.2 – UTILIZAÇÃO DOS MEIOS FÍSICOS GUIADOS

Os meios físicos utilizados antes da década de 1980 não eram padronizados. Cada fabricante adotava seu modelo em um projeto de cabeamento e fornecia orientação quanto à instalação do seu tipo de cabo. Dessa forma, tornava-se difícil ao instalador compreender as diversas técnicas de cada fabricante e a interação dos componentes. Para modificar esse panorama, vários órgãos, como por exemplo, IEEE (Institute of Electrical and Electronic Engineers – Instituto de Engenheiros Eletricistas e Eletrônicos) e EIA (Eletronic Industries Alliance – Aliança das Indústrias Eletrônicas), se reuniram para propor e especificar os parâmetros para os cabos e acessórios utilizados em um sistema de cabeamento estruturado.

Ethernet e Token Ring são classificações de arquiteturas de rede. As redes Token Ring foram concebidas pela IBM, mas como os custos dos seus equipamentos eram muito altos, acabaram caindo em desuso. Já as redes Ethernet evoluíram muito, por terem adotado um padrão aberto, o que abriu o mercado para vários fabricantes produzirem equipamentos para este modelo, como hubs, switches, roteadores, tomadas e cabos. Atualmente, mais de 90% das redes locais instalados no mundo são da arquitetura Ethernet, o IEEE padronizou esta rede sob o número 802.3.

15.3 – TIPOS DE MEIOS FÍSICOS GUIADOS

Vários meios físicos podem ser utilizados para realizar a transmissão de dados, cada um com propriedades específicas. São basicamente agrupados em fios de cobre (como o par trançado e o cabo coaxial) e ópticos (como as fibras ópticas).

Vamos falar sobre o cabo par trançado e sua confexão, pois é o mais usado.

15.3.1 – PAR TRANÇADO

Os cabos de par trançado atualmente possuem 4 pares dispostos dentro de uma proteção externa de PVC. Cada par é formado por dois fios entrelaçados. Esse cabo consiste em dois fios entrelaçados em forma helicoidal (figura 37).

Com os fios dispostos em forma de par trançado, as ondas geradas pelos diferentes pares de fios tendem a se cancelar, o que significa menor interferência.

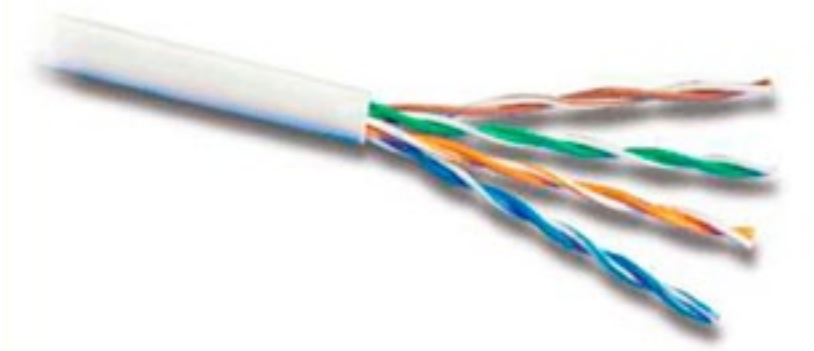

Figura 37- Cabo Par Trançado com 4 pares.
Fonte: http://www.mandarino.pro.br/Sites/NovoRedes/images/utp2.gif

Essa proteção contra interferência eletromagnética não é o único tipo de proteção que um cabo par trançado pode oferecer. Esses cabos podem ainda apresentar uma proteção adicional contra interferências. Em função disso, existem dois tipos de par trançado:

- **STP (Shielded Twisted Pair – Par Trançado Blindado):** esse tipo de cabo possui em volta dos pares uma espécie de papel alumínio. Essa proteção de alumínio serve como uma blindagem adicional contra interferências externas, como motores elétricos, reatores de lâmpadas e equipamentos industriais, que geram ondas eletromagnéticas que podem corromper os dados que trafegam pelo cabo.
- **UTP (Unshielded Twisted Pair – Par Trançado Não Blindado):** esse é o cabo mais simples e mais barato para as redes locais. É conhecido popularmente como "cabo de internet", já que as pessoas têm o hábito de compartilhar internet com os vizinhos utilizando esse cabo. É ainda o mais utilizado para montar redes locais nas empresas.

Figura 38 - Cabo Par Trançado STP.
Fonte: http://www.rapidoinfoshop.com.br/blog/wp-content/fotos/11-2010/Cabos-Conectores-UTP/11.jpg

Figura 39 - Cabo Par Trançado UTP.
Fonte: http://www.digel.com.br/novosite/images/stories/cat5.jpg

Esse tipo de cabo necessita de um conector para se ligar às interfaces de rede ou às portas dos switchs do tipo RJ-45. Eles são instalados nas pontas dos cabos, utilizando uma ferramenta de "crimpagem".

Figura 40 - Conector RJ-45 Crimpado no Cabo.
Fonte: http://rcinfopage.hd1.com.br/imagens/rj45.jpg

15.4 – EXERCÍCIOS PROPOSTOS

1) Para que serve os meios físicos de transporte guiados?

_____
_____
_____

2) Quais os tipos de par trançado? Defina-os.

_____
_____
_____

16 - MEIO FÍSICO DE TRANSMISSÃO II

No capítulo anterior vimos um dos principais meios físicos de transmissão do tipo "guiado", que utilizam cabos. Neste capítulo verificaremos as principais formas não guiadas de transmissão, que utilizam o ar como meio físico.

16.1 – INTRODUÇÃO

Prédios antigos ou empresas com escritórios situados em prédios diferentes, aeroportos e rodoviárias são situações, não únicas, comuns para utilização de algum tipo de enlace sem fio.

A ideia das comunicações sem fio não é substituir por inteiro as redes de cabeamento, mas fornecer opções e flexibilidade de uso por parte do utilizador. Vamos ver a serguir os principais sistemas de transmissão de dados sem fio.

16.2 – UTILIZAÇÃO DOS MEIOS FÍSICOS NÃO GUIADOS

Para a utilização de um enlace de comunicação sem fio, faz-se necessário o uso de transmissores e receptores que se comuniquem através de frequências lançadas no ar.

> *Quando se instala uma antena com o tamanho apropriado em um circuito elétrico, as ondas eletromagnéticas podem ser transmitidas e recebidas com eficiência por um receptor localizado a uma distância bastante razoável. Toda comunicação sem fio é baseada nesse princípio. (TANEMBAUM, 2003)*

Medição de Frequência é o agrupamento de frequências que adota notação de potências de 10 (diferentemente da informática, que usa muito potências de 2). Observe:

1 KHz = 1000 Hz ou 103 Hz
1 MHz = 1000 KHz ou 103 KHz
1 gHz = 1000 MHz ou 103 MHz

As redes sem fio, tanto em nossas residências como em locais públicos, também necessitam de um transmissor. Em todas elas é comum observarmos a existência de um aparelho que forneça o enlace sem fio (chamado de AP – Access Point – Ponto de Acesso) dotado de uma antena e a existência de um computador ou notebook dotado de uma interface de rede wireless (sem fio).

As interfaces de rede sem fio dos notebooks e netbooks estão localizadas na placa mãe do aparelho, normalmente num slot mini-pci, as antenas estão ligadas a essa interface e costumam ficar localizadas nas extremidades direita e esquerda da tela de LCD do aparelho (na parte de dentro).

16.3 – TIPOS DE MEIOS FÍSICOS NÃO GUIADOS

A transmissão por radiofrequência não é a única forma para os enlaces sem fio. Dependendo da aplicação que se deseja atender ou o serviço a ofertar, um enlace diferente pode ser utilizado, mas sem dúvida, a radiofrequência é um dos enlaces sem fio mais utilizada. Vejamos os principais.

16.3.1 – RÁDIO, RF OU RADIOFREQUÊNCIA

As ondas de rádio são fáceis de gerar e conseguem percorrer longas distâncias e atravessar prédios e paredes. Devido a essas características, elas são amplamente utilizadas. Existem

dois modos básicos de transmissão em RF: as ondas que se propagam de forma difusa (ou omnidirecionais – que se propagam em todas as direções, possibilitando várias conexões) e as ondas que se propagam de forma direcional, formando apenas um enlace. Os governos controlam o licenciamento de uso, justamente para evitar que algumas frequências interfiram em outras. Todas as bandas de celulares, canais de rádio e TV, Sistemas de Posicionamento Global (GPS) e radar de controle de tráfego aéreo, dentre outras, são controladas pelos governos.

Banda - quando usamos o termo banda para RF, estamos nos referindo ao intervalo de frequências que aquela transmissão pode utilizar, por exemplo, a banda para as rádios FM pode variar de 88 a 174 Mhz; os sistemas GPS possuem banda no intervalo de 1227 a 1575 Mhz. Como as transmissões de TV ocupam parte da banda FM, talvez você tenha visto algum aparelho de rádio que permite ouvir o som de transmissões de TV.

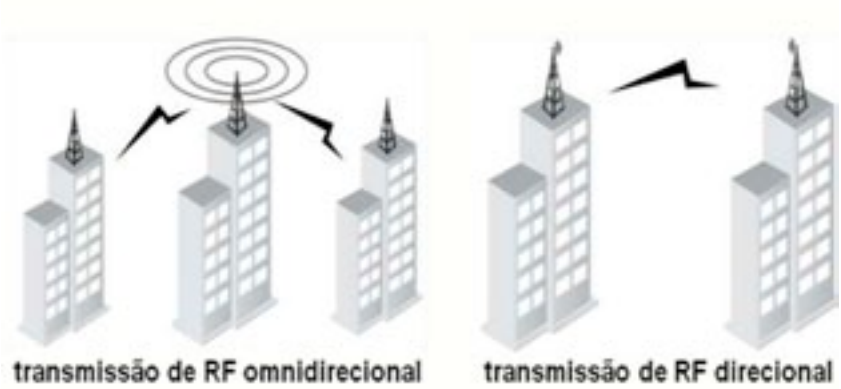

Figura 41 - RF Omnidirecional e RF Direcional.
Fonte: Rede de Computadores / Allan Francisco Forzza Amaral p.73

16.3.2 – MICRO-ONDAS

Quando há necessidade de transmissão de dados em longas distâncias, o enlace micro-ondas é mais eficaz, podendo chegar a taxas de 1 Gbps. Esse sistema é chamado também de MMDS (Multipoint Microwave Distribution System – Sistema de Distribuição Multiponto Micro-ondas) e utiliza antenas direcionais para estabelecer o enlace. A frequência neste tipo de transmissão normalmente precisa ser licenciada pelo órgão regulador do governo (no caso do Brasil, a ANATEL).

Figura 42 - Transmissão num sistema direcional micro-ondas.
Fonte: http://www.sistemaplug.com.br/img/institucional_sisplug/mmds.jpg

16.3.3 – LASER

Outra forma de transmissão sem fio é o sinal óptico sob forma de laser, que já vem sendo utilizado há algum tempo. O mais comum nesse tipo de enlace é a conexão de LAN's situadas em prédios diferentes, porém com visada. Uma das vantagens desse tipo de transmissão é prescindir (não necessitar) da licença de um órgão regulador. E uma das desvantagens é a natureza direcional: é necessário precisão milimétrica para estabelecer a visada perfeita. Muitas vezes são usadas lentes que desfocam o laser para facilitar o estabelecimento do enlace.

LASER (Light Amplification by Stimulated Emission of Radiation) – É a amplificação da luz por emissão estimulada de radiação. É um dispositivo que produz radiação eletromagnética monocromática através de um feixe de luz de aproximadamente 1 mm de largura.

Mesmo sendo o custo relativamente baixo, esse tipo de enlace enfrenta alguns problemas, o primeiro deles é a natureza direcional, que é necessário precisão milimétrica para estabelecer a mira perfeita. Muitas vezes são usadas lentes que desfocam o laser para facilitar o estabelecimento do enlace. Outro fato é a questão do tempo, há problemas na transmissão em dias de chuva e de neblina; também em dias de sol intenso pode haver interferências das correntes de convecção (turbulências de ar quente) que emanam dos telhados e desviam o feixe de laser.

16.4 – EXERCÍCIO PROPOSTO

1) Para que serve os meios físicos de transporte não guiados? Dê exemplo.

_____
_____
_____

17 - PADRÕES DE REDE

Neste capítulo voltaremos a falar sobre alguns padrões já consagrados na produção dos componentes das redes. O conhecimento desses padrões nos permite selecionar mais convenientemente os equipamentos que utilizaremos na montagem e configuração de nossas redes.

17.1 – INTRODUÇÃO

Vimos em capítulo anterior uma breve descrição das camadas do modelo atual de padronização das redes. Explicamos que o modelo é apenas uma referência, daí o nome RM-OSI (Reference Model – Modelo de Referência OSI). O modelo agrupa as funções necessárias ao funcionamento das redes em sete camadas. De acordo com a finalidade de cada uma das camadas, podemos novamente classificá-las em três grandes grupos:

- **Grupo REDE:** formado pelas camadas FÍSICA, ENLACE e REDE.
- **Grupo TRANSPORTE:** com apenas a camada de TRANSPORTE.
- **Grupo APLICAÇÃO:** abrangendo as camadas SESSÃO, APRESENTAÇÃO e APLICAÇÃO.

Existem dois padrões que são muito importantes: O modelo da arquitetura Ethernet e o modelo da arquitetura TCP/IP. Aqui estudaremos o modelo Ethernet.

17.2 – PADRÃO IEEE

O IEEE (lê-se i3é – Institute of Electrical and Electronic Engineers – Instituto de Engenheiros Eletricistas e Eletrônicos) foi inicialmente apresentado no capítulo antetior. Sua finalidade é colaborar no incremento da prosperidade mundial, promovendo a engenharia de criação, desenvolvimento, integração e o compartilhamento do conhecimento aplicado no que se refere à ciência e às tecnologias da eletricidade e da informação, em benefício da humanidade e da profissão.

Criado em 1984, nos EUA, o IEEE é uma sociedade técnico-profissional internacional, dedicada ao avanço da teoria e prática da engenharia nos campos da eletricidade, eletrônica e computação. Existem vários padrões do IEEE como mostra a figura abaixo:

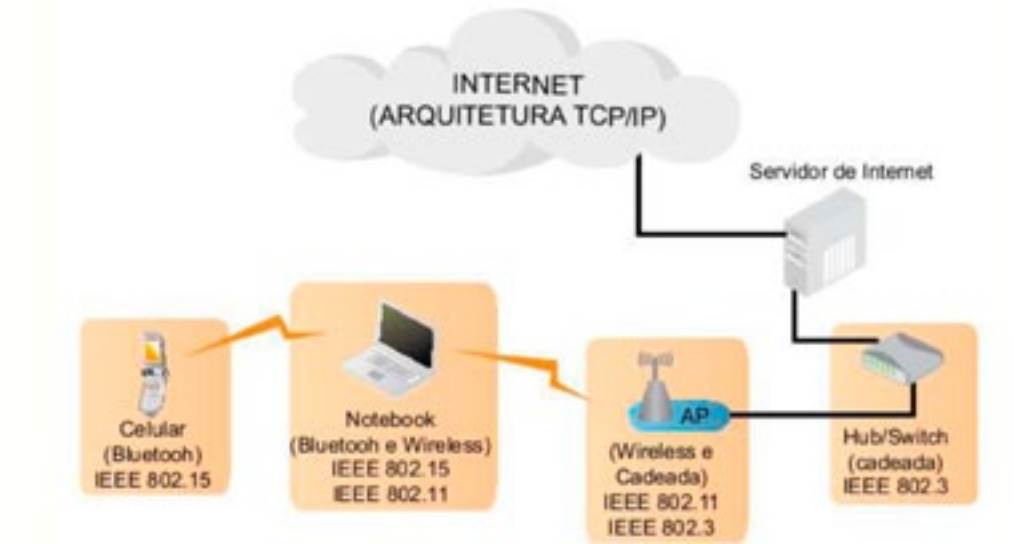

Figura 43 - Comunicações entre redes IEEE diferentes.
Fonte: Rede de Computadores / Allan Francisco Forzza Amaral p.81

O modelo Ethernet, relacionado às duas camadas iniciais do modelo OSI, segue uma pilha de protocolos conforme figura abaixo.

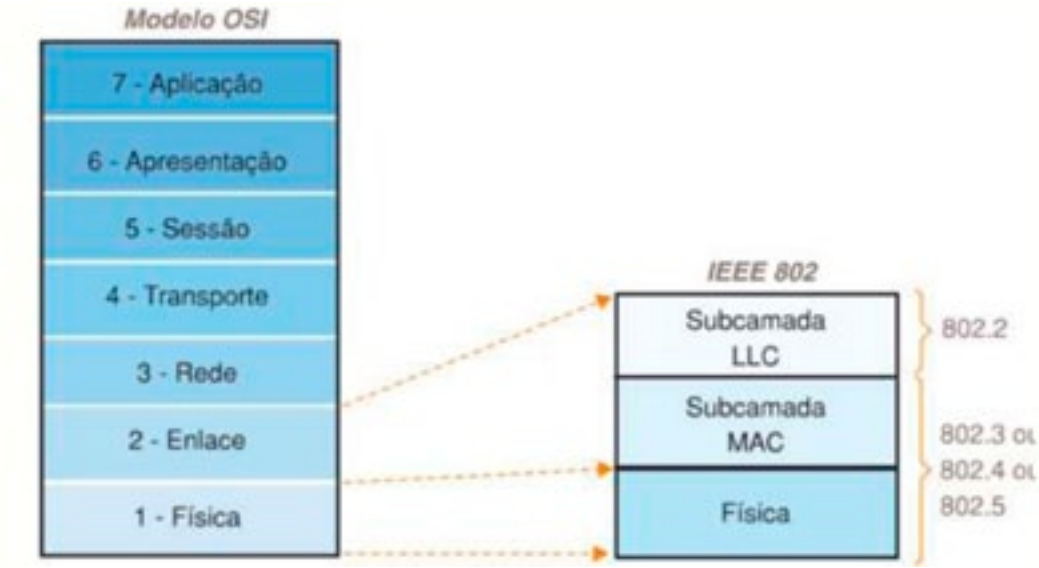

Figura 44 - Ethernet em relação à RM-OSI.
Fonte: http://www.mecatronicaatual.com.br/files/image/ethernet_figura_02_5_.jpg

O modelo de arquitetura Ethernet não é o único criado pelo IEEE, é apenas o mais famoso devido à sua utilização em massa. A sua padronização fez com que muitos fabricantes de equipamentos desse modelo concorressem entre si, fazendo os preços caírem e obviamente aumentando o consumo.

17.2.1 – IEEE 802.3, IEEE 802.3U, IEEE 802.3AB, IEEE 802.3Z

Vamos ver alguns dos seus principais identificadores e significados:

a) IEEE 802.3 (ou 10BASE-T): transmissão de dados a uma taxa de 10 Mbps, utilizando banda básica (BASE) e cabo par trançado (T, de twisted pair – par CAT3 ou superior).
b) IEEE 802.3u (ou 100BASE-T): **idem acima, porém, com taxa de 100 Mbps e cabo par** trançado CAT5 ou superior.
c) IEEE 802.3ab (ou 1000BASE-CX): transmissão de dados à taxa de 1000 Mbps, utilizando cabo de cobre (par trançado) a uma distância máxima de 25 metros, padrão muito pouco utilizado.
d) IEEE 802.3z (ou 1000BASE-LX): transmissão a 1000 Mbps utilizando cabos de fibras ópticas monomodo.
e) IEEE 802.3z (ou 1000BASE-SX): transmissão a 1000 Mbps utilizando cabos de fibras ópticas multimodo.

17.2.2 – IEEE 802.11

As redes sem fio IEEE 802.11, também conhecidas como redes Wi-Fi ou Wireless, foram uma das grandes novidades tecnológicas dos últimos tempos. O padrão divide-se em várias partes, sendo as principais:

- **802.11b:** a principal característica dessa versão é a possibilidade de estabelecer conexões nas seguintes taxas de transmissão: 1, 2, 5.5 e 11 Mbps. O intervalo de frequências é o mesmo utilizado pelo 802.11 original (entre 2,4 e 2,4835 gHz).

A área de cobertura de uma transmissão 802.11b pode atingir 400 metros em ambientes abertos e 50 metros em lugares fechados.

- **802.11a:** sua principal característica é a possibilidade de operar com as seguintes taxas de transmissão de dados: 6, 9, 12, 18, 24, 36, 48 e 54 Mbps. O alcance geográfico de sua transmissão é de cerca de 50 metros. A sua frequência de operação é diferente do padrão 802.11 original: 5 GHz. Devido à sua faixa de frequência, este padrão é pouco utilizado.
- **802.11g:** o padrão 802.11g foi disponibilizado em 2003 e é tido como o sucessor natural da versão 802.11b, uma vez que é totalmente compatível com este. O principal atrativo do padrão 802.11g é poder operar com taxas de transmissão de até 54 Mbps, assim como acontece com o padrão 802.11a. Funciona com frequências na faixa de 2,4 GHz e possui praticamente o mesmo poder de cobertura do seu antecessor, o padrão 802.11b.
- **802.11n:** sua principal característica é o uso de um esquema chamado Multiple-Input Multiple-Output (MIMO – Múltiplas Entradas e Múltiplas Saídas). Assim, é possível usar dois, três ou quatro emissores e receptores para o funcionamento da rede. Uma das configurações mais comuns neste caso é o uso de APs que utilizam três antenas (três vias de transmissão). O padrão 802.11n é capaz de fazer transmissões na faixa de 300 Mbps e pode trabalhar com frequências na faixa de 2,4 GHz a 5 gHz, o que o torna compatível com os padrões anteriores, inclusive com o 802.11a.

17.2.3 – IEEE 802.16

As redes sem fio IEEE 802.16 para serem utilizadas em redes metropolitanas sem fio (wireless MAN ou WMAN) são mais conhecidas como WiMAX (Worldwide Interoperability for Microwave Access – Interoperabilidade Extensa/Mundial de Acesso por Micro-ondas). A WMAN oferece uma alternativa para redes cabeadas, como enlaces de fibra óptica, sistemas coaxiais, utilizando cable modems (modens a cabo) e enlaces de acesso banda larga, como DSL (Digital Subscriber Line – Linha Digital do Assinante).

Figura 45 - Transmissão de dados na tecnologia WiMax.
Fonte: http://s3.amazonaws.com/magoo/ABAAAAMMUAF-2.png

O IEEE 802.16 é uma tecnologia extremamente interessante para a cobertura de áreas remotas e pontos de difícil acesso, localidades, enfim, que não tenham acesso à rede cabeada. Redes metropolitanas têm uma cobertura com alcance de algumas dezenas de quilômetros. Alguns fatores trazem dificuldades adicionais e podem ser críticos para o bom funcionamento de uma rede sem fio desse porte, como:

- Necessidade de visada direta, o que dificulta os ajustes das antenas.
- Número de usuários atendidos simultaneamente.
- Segurança.

17.3 – EXERCÍCIO PROPOSTO

1) O que são padrões de rede e para que servem? Dê exemplo.

_____
_____
_____

18 - CONFIGURAÇÃO DE REDE LÓGICA

Nos capítulos anteriores vimos a parte física de uma rede, agora vamos falar um pouco da parte lógica, pois para uma rede funcionar direito precisa da parte física e lógica instaladas corretamente.

18.1 – INTRODUÇÃO

Estudamos até agora como instalar a parte física de uma rede, mas não é somente a passagem dos cabos e a parte elétrica que faz com que os micros troquem informações entre si, precisamos além de protocolos que vimos no item anterior, configurar o SERVIDOR e ESTAÇÕES de TRABALHO utilizando software de rede, como mencionado no item 3.4 do Capítulo 3, para concluir nossa rede, onde:

- **Servidor:** micro que centraliza as informações e fornece as senhas para os usuários.
- **Estação de Trabalho:** onde o usuário executa os trabalhos.

18.2 – REDE CLIENTE/SERVIDOR

Neste tipo de sistema, temos computadores centrais que funcionam o tempo todo apenas fornecendo serviços para a rede e temos computadores clientes ou usuários que usufruem dos serviços fornecidos pelo servidor.

Figura 46 - Rede Cliente/Servidor.
Fonte: http://penta2.ufrgs.br/redes296/cliente_ser/image.gif

18.3 – REDE PONTO A PONTO

Neste sistema, todos os computadores são tanto servidores de recursos para a rede, quanto cliente dos serviços fornecidos pelos outros computadores.

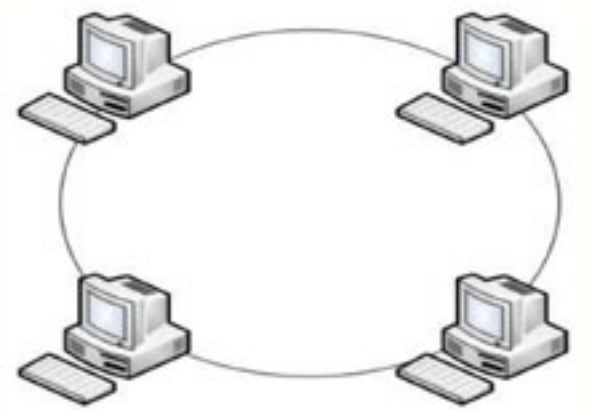

Figura 47 - Rede Ponta a Ponto.
Fonte: http://fapers.hdfree.com.br/_conteudo/_informatica/_modulo1/_sor/_imagens/_ta.jpg

18.4 – EXEMPLO DE CONFIGURAÇÃO LÓGICA COM O WINDOWS XP

A primeira coisa que devemos entender é que o windows XP tem definições de usuários e senhas. Todos os usuários que tenham acesso ao servidor devem ser cadastrados no servidor, com seus direitos ou restrições, lembrando que mostraremos aqui um processo básico.

18.4.1 – CRIANDO CONTO DO USUÁRIO

Para criarmos contas de usuários temos duas opções no XP. A primeira é a opção contas de usuários no painel de controle, esta opção oferece uma interface mais amigável, é ideal para usuários que estão começando a estudar e a lidar com contas de usuários e grupos.

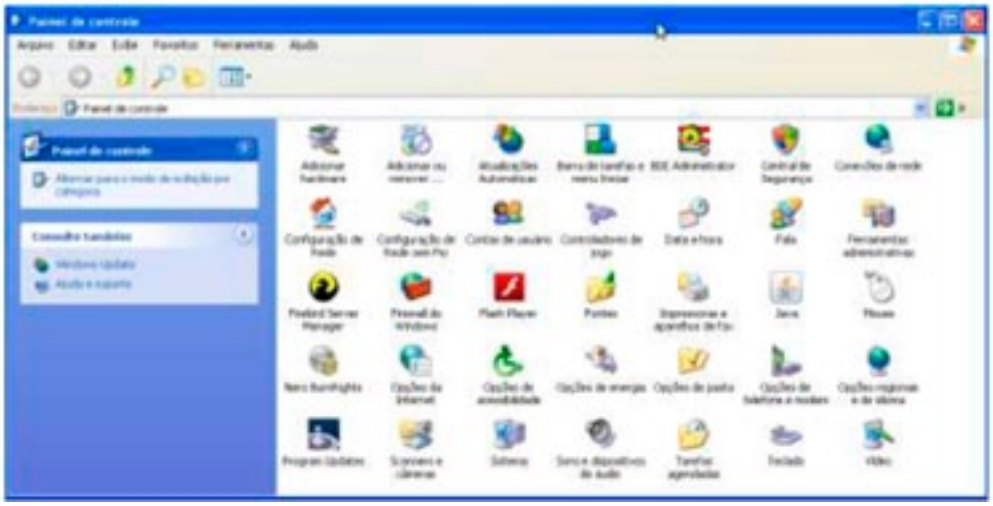

Figura 47 - Painel de Controle do Windows XP.
Fonte: Criada pelos autores

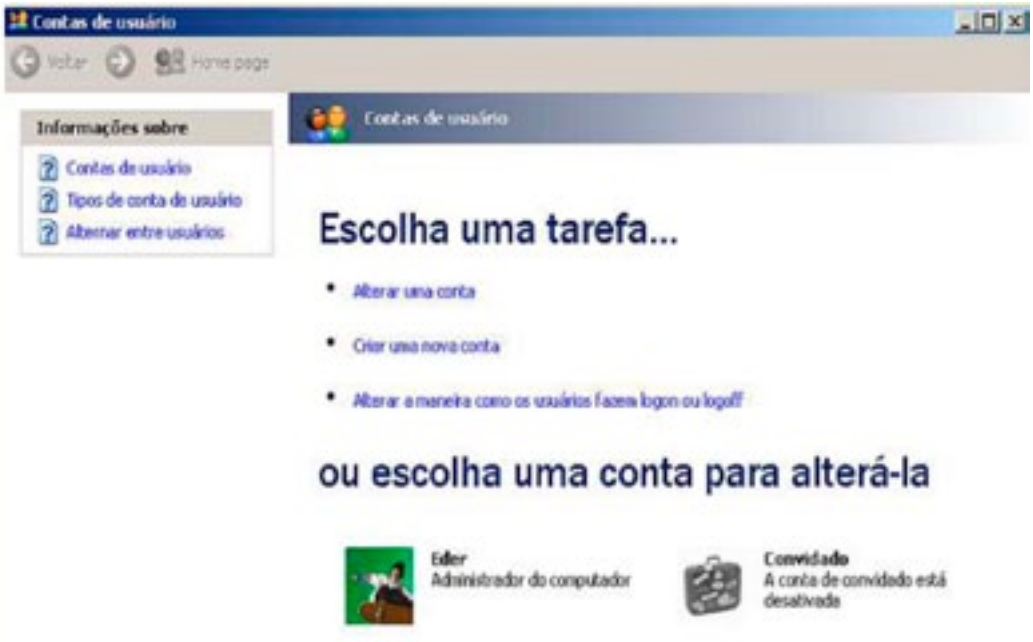

Figura 48 - Tela das Contas de Usuário.
Fonte: Criada pelos autores

Após clicar em contas de usuário no painel de controle, podemos criar uma nova conta, alterar uma já existente e alterar a forma de logon e logof do usuário. Vamos clicar no item criar nova conta.

Contas de usuário
Voltar
Home page
Dê um nome para a nova conta
Digite um nome para a nova conta:
novaconta
Este nome será mostrado na tela de boas-vindas e no menu 'Iniciar'.
Avançar >
Cancelar

Figura 49 - Tela de Criar Nova Conta.
Fonte: Criada pelos autores

Nesta tela colocaremos o nome da nova conta de usuário. E clicamos em avançar.

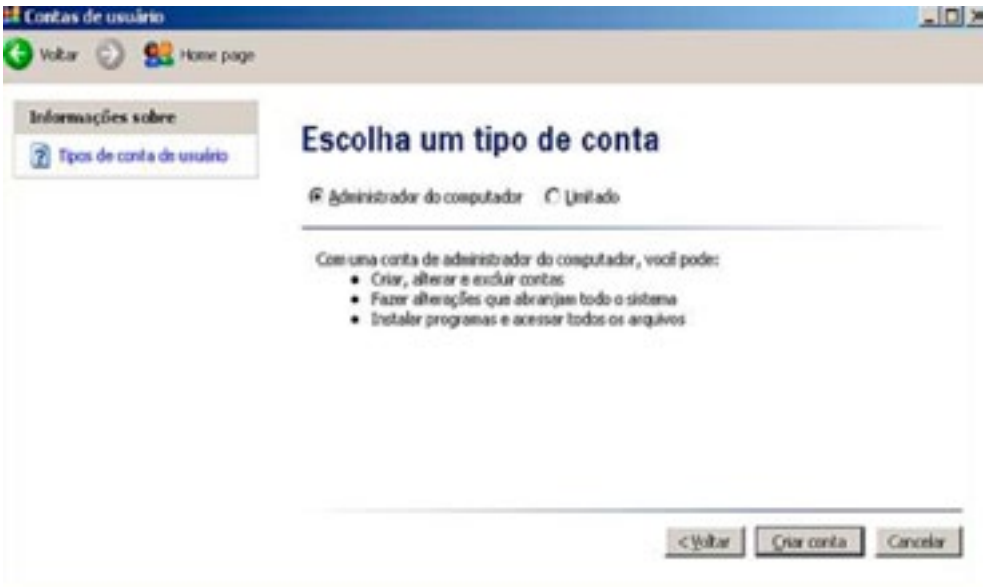

Figura 50 - Tela do Tipo de Conta.
Fonte: Criada pelos autores

Nesta tela, o usuário clicará em uma das opções: Administrador do Computador ou Limitado. Os usuários limitados não terão direitos para instalar determinados programas, necessitando utilizar uma senha do administrador, já o administrador terá direitos totais. Para finalizar clicamos em Criar Conta.

18.5 – EXERCÍCIO PROPOSTO

1) Em configuração de rede lógica, quais os tipos existentes? Explique-os.

_____
_____
_____

19 - POLÍTICA DE SEGURANÇA

Neste capítulo iremos falar um pouco sobre política de segurança para os computadores interligados na rede e seus inimigos, os crackers.

19.1 – CONCEITO

Política de segurança não é nada mais que uma declaração formal das regras que as pessoas que possuem um determinado acesso à tecnologia e aos ativos de informações de uma empresa devem obedecer.

19.2 – PRINCÍPIOS DE SEGURANÇA

Figura 51 - Princípios de Segurança.
Fonte: Criada pelos autores

Figura 52 - Segurança de Informação.
Fonte: Criada pelos autores

Segundo Bruce Schneier, "segurança é uma corrente: ela é tão segura quanto seu elo mais fraco."

Para se proteger de algo você precisa pensar como eles, os crackers:

- Quem são seus inimigos?
- Que ferramentas utilizam?
- Como agem?
- Quais são seus objetivos?

Cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por hackers em defesa contra o uso jornalístico do termo hacker. O uso deste termo reflete a forte revolta destes contra o roubo e vandalismo praticado pelo cracking.

19.3 - TIPOS DE CRACKERS

1. Crackers de Criptografia: termo usado para designar aqueles que se dedicam à quebra de criptográfia (cracking codes). Tal procedimento pode ser executado tanto com lápis e papel, bem como com uso de computadores, tudo depende da fonte do problema a ser solucionado.

2. Crackers de Softwares: termo usado para designar programadores e decoders que fazem engenharia reversa de um determinado programa, ou seja, alteram o conteúdo de um determinado programa pra fazer funcionar de forma correta. Muitos crackers alteram datas de expiração de um determinado programa para fazer funcionar mais de 30 dias, ou seja, modificam o modo trial para utilizar como se fosse uma cópia legítima, ou fazem um desvio interno na rotina de registro do programa para que ele passe a aceitar quaisquer seriais, tais sofwares alterados são conhecidos como warez.

3. Desenvolvedores de vírus, worms, trojans e outros malwares: programadores que criam pequenos softwares que causam danos ao usuário.

19.4 – FILOSOFIAS DA POLÍTICA

- Tudo o que não for expressamente PERMITIDO está PROIBIDO.
- Tudo o que não for expressamente PROIBIDO está PERMITIDO.

19.5 – OS OBJETIVOS DE PREOCULPAÇÕES

- Serviços x Segurança fornecida.
- Facilidade de uso x Segurança.
- Custo da segurança x Risco da perda

19.6 – CARACTERÍSTICAS DA BOA POLÍTICA

- Deve ser implementada.
- Deve ser divulgada.
- Deve utilizar ferramentas de segurança.
- Deve prever punições.
- Deve claramente definir responsabilidades para os usuários, administradores e gerentes.

19.7 – COMPONENTES DA BOA POLÍTICA

- Análise dos riscos (identificar quais os bens que você quer proteger e identificar as ameaças).
- Política de desenvolvimento (interno e externo) e aquisição de sistemas.
- Política de privacidade.
- Política de acesso.
- Política de responsabilidades.
- Política de autenticação (política de senhas).
- Política de disponibilidade.
- Política de manutenção da rede e sistemas.
- Política de violações (internas e externas).
- Política de suporte ao usuário.
- Política de treinamento.
- Manutenção e auditoria.

OBS.: Lembrando que não existe sistema 100% seguro.

19.8 – EXERCÍCIO PROPOSTO

1) Quais são os tipos de Crackers?

_____
_____
_____

20 - SISTEMA OPERACIONAL WINDOWS NT

Neste capítulo iremos falar um pouco sobre o S.O. (Sistema Operacional) Windows NT, característica de S.O. de rede e a evolução da família Windows.

20.1 – INTRODUÇÃO

Os sistemas operacionais de rede tiveram uma longa caminhada desde os tempos em que eram simplesmente servidores para serviços de arquivos e impressão até chegarem aos NOS's (Network Operating Systems - Sistemas Operacionais de Rede), um ambiente operacional de rede completo, que sustenta e suporta as aplicações ao mesmo tempo em que torna invisíveis as conexões entre os recursos. O Windows NT (New Technology) é um ramo separado da família Windows.

O NT possui recursos multitarefas integrais que faltam ao Windows. Isso significa que o computador pode executar diversas tarefas, incluindo comunicações, de uma só vez sem falhas. O pacote do servidor NT também oferece mais segurança do que o Windows. Tanto o Windows como o Windows NT fazem uso extensivo das operações em 32 bits para mover rapidamente os dados dentro do computador.

Figura 53 - Sistema Operacional Windows NT.
Fonte: http://2.bp.blogspot.com/-LAzmB0rlKoQ/TzMdiJuZFQI/AAAAAAAACEM/O8aDulkuziI/s1600/111_1996b_ms_windows_nt_server_4_0.jpg

20.2 – CARACTERÍSTICA DO SOFTWARE

O talento para rodar, de modo eficiente, messaging, base de dados e outras aplicações baseadas em um servidor numa rede cliente/servidor é um requisito fundamental da maior parte das redes modernas. O suporte a processadores múltiplos é aqui um ingrediente essencial, assim como é a tolerância a falhas, ferramentas de alta qualidade para desenvolvimento e suporte às aplicações por parte de vendedores terceiros.

20.3 – CARACTERÍSTICA DO HADWARE

Se o sistema não funciona com o hardware que temos, que desejamos ou para o qual pretendemos migrar, então não nos serve, inclui a facilidade de utilização dos protocolos de transporte de rede e a possibilidade de o servidor lidar com múltiplos adaptadores de LAN e com o roteamento interno. Tanto o tipo de processador como a capacidade para utilizar mais de um são fatores importantes.

20.4 – FAMÍLIA DO WINDOWS

- Windows 1.0
- Windows 2.0
- Windows 3.1
- Windows 95
- Windows 98
- Windows ME
- Windows 2000 (Tecnologia NT)
- Windows XP
- Windows Vista
- Windows 7

20.5 – EXERCÍCIO PROPOSTO

1) Cite algumas características do Windows NT.

_____
_____
_____

21 - SISTEMA OPERACIONAL LINUX

Neste capítulo iremos falar um pouco sobre o Sistema Operacional Linux e a evolução de uma determinada distribuição do Linux chama-se Ubuntu.

21.1 – INTRODUÇÃO

O Linux é um tipo de Unix criado por hackers com uma alternativa barata e funcional para quem não está disposto a pagar alto preço de um sistema Unix ou não tem um computador rápido o suficiente. O Linux foi primeiramente desenvolvido para PC's baseados em 386/486/Pentium, mas atualmente também roda nos computadores com processadores da atualidade.

- O Linux foi escrito inteiramente do nada, não há código proprietário em seu interior.
- O Linux está disponível na forma de código objeto, bem como em código fonte aberto.

Figura 54 - Sistema Operacional Linux Ubuntu.
Fonte: http://upload.wikimedia.org/wikipedia/commons/8/87/Ubuntu_Linux_6.06.png

21.2 – CARACTERÍSTICAS

O Linux possui todas as características que você pode esperar de um sistema operacional, incluindo:

- Multitarefa real.
- Memória virtual.
- Biblioteca compartilhada.
- Gerenciamento de memória própria.
- Executáveis "copy-on-write" compartilhados.
- Rede TCP/IP (incluindo SLIP/PPP/ISDN).
- X Windows.

21.3 – HISTÓRICO

Diferente do Windows XP ou do NT, o Sistema Operacional Linux não é um produto único, pelo contrário, existem muitas versões distribuídas no mercado, tais como:

- Red Hat
- Conectiva
- Ubuntu
- Debian
- Etc.

21.4 – EVOLUÇÃO DO UBUNTU

- Ubuntu 4.10
- Ubuntu 5.04
- Ubuntu 5.10
- Ubuntu 6.06
- Ubuntu 6.10
- Ubuntu 7.04
- Ubuntu 7.10
- Ubuntu 8.04
- Ubuntu 8.10
- Ubuntu 9.04
- Ubuntu 9.10
- Ubuntu 10.04
- Ubuntu 10.10
- Ubuntu 11.04
- Ubuntu 11.10
- Ubuntu 12.04

21.5 – EXERCÍCIOS PROPOSTOS

1) Site algumas características do Linux.

_____
_____
_____

2) Descreva algumas evoluções do Linux Ubuntu.

_____
_____
_____

22 - LINUX X WINDOWS

No capítulo anterior vimos dois Sistemas Operacionais, suas histórias e evoluções. Neste capítulo iremos falar um pouco sobre a diferença do S.O. Linux em relação ao S.O. Windows.

22.1 – INTRODUÇÃO

Existem vários outros sistemas para as plataformas suportadas pelo Linux, particularmente para as máquinas Intel, embora sem sombra de dúvidas, a Microsoft (http://www.microsoft.com/) e seus Sistemas Operacionais Windows dominem o mercado com uma larga vantagem sobre seus concorrentes. Mas o que o Linux pode oferecer em comparação às alternativas disponíveis, tanto comercialmente quanto gratuitas?

22.2 – WINDOWS

Em todas as suas versões (Windows Original, Windows 98 e Windows XP), o sistema gráfico da Microsoft não consegue evitar muitos dos problemas inerentes à sua base operativa inicial, o MS-DOS. Embora ofereça uma interface bastante amigável e suporte para rede nativo, ainda é um sistema extremamente frágil, novamente uma consequência da necessidade de back-compatibility exigida pelo mercado.

Figura 55 - Windows XP.
Fonte: http://3.bp.blogspot.com/_Y6-0h6rX7i8/TNTW8U975sI/AAAAAAAAASg/S68LIsiw8a0/s1600/windows_xp_logo.jpg

22.3 – WINDOWS NT

O Windows NT desde seu lançamento vem sendo promovido pela Microsoft como uma alternativa aos sistemas Unix. O primeiro sistema operacional da Microsoft disponível para múltiplas plataformas (Alpha e Intel x86, entre outras) oferece muitos dos recursos que fazem parte de qualquer sistema POSIX do mercado há bastante tempo, com o grande problema do pouco tempo de maturação. Além disso, o Windows NT possui a grande desvantagem de ter o seu ambiente gráfico acoplado de tal forma ao sistema operacional que se torna praticamente impossível operar um console sem o overhead causado pela interface gráfica, exigindo máquinas bem mais poderosas para executar as mesmas tarefas que as alternativas, mesmo as comerciais.

Figura 56 - Windows 2000 Server (Família do NT).
Fonte: http://www.guidebookgallery.org/pics/gui/startupshutdown/splash/win2000advserv.png

22.4 – LINUX

O Linux é um sistema operacional do tipo Unix. O padrão System V está embutido no seu Kernel, foi desenvolvido para a plataforma IBM-PC, sendo assim, ele possui a robustez, segurança e flexibilidade do Unix. Além disso, ele já possui uma interface gráfica nas suas novas distribuições, por exemplo, o Ubuntu. Existem outras interfaces gráficas que são semelhantes as do Windows, menos sofisticadas, menos aplicativas e menos elaboradas, porém muito funcionais.

Figura 57. Linux
Fonte: http://www.tecnologiaetreinamento.com.br/wp-content/uploads/2010/04/instalacao-linux.jpg

22.5 – EXERCÍCIO PROPOSTO

1) Cite algumas diferenças do Linux em relação ao Windows.

_____
_____
_____

23 – FUTURO DAS REDES

Neste capítulo falaremos um pouco sobre o futuro das redes de computadores, principalmente da rede mundial, a Internet.

23.1 – INTRODUÇÃO

As redes de computadores têm crescido muito, em tamanho e em complexidade. O acesso a qualquer tipo de rede de dados antigamente era restrita a um grupo de pessoas, composto por cientistas, pesquisadores, tecnólogos e militares. Hoje em dia, as redes de computadores tornaram-se parte essencial de nossa infraestrutura. O crescimento rápido da Internet talvez seja um dos mais interessantes fenômenos nesta área. Dentre os fatores que contribuíram para tal crescimento, destaca-se o protocolo de comunicação, o Internet Protocol ou simplesmente "IP".

23.2 – IPV4

Essa versão atual do protocolo IPv4 tem sido extremamente bem-sucedida. A sua utilização possibilitou à Internet lidar com redes de dados heterogêneas, com o constante avanço tecnológico dos equipamentos e com a alta escalabilidade.

Figura 58 - IPv4.
Fonte: http://info.menandmice.com/Portals/77026/images/bigstock_Browse_Local_On_____6191537-resized-600.jpg

23.3 – IPV6

A nova versão, conhecida como IPv6 ou IPng (Next Generation), surge como uma resposta à deficiência do IPv4. O IPv6 disponibiliza 128 bits para endereçamento (ao invés dos 32 da versão antiga), suficientes para se obter 1.564 endereços distintos por m² do planeta Terra. Com a capacidade expandida de endereçamento é, até certo ponto, compatível com o atual padrão, o que deverá suavizar o processo de transição.

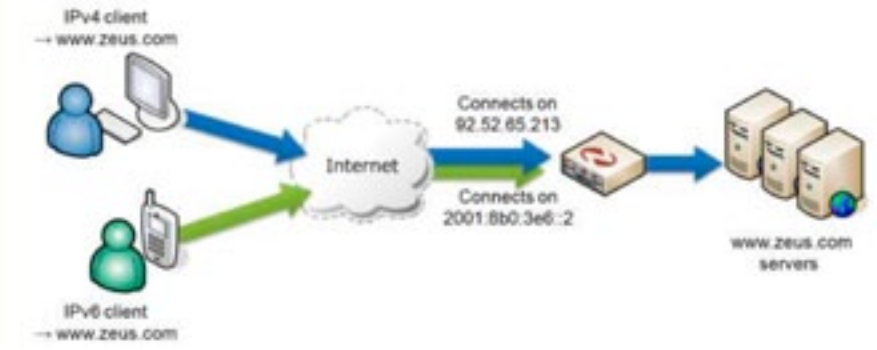

Figura 59 - IPv6.

Fonte: http://www.aidoweb.com/images/upload/pouzy/ipv6_1.png

Dentre as principais melhorias trazidas por essa versão, podemos destacar as seguintes:

- Extensão das capacidades de endereçamento e roteamento de pacotes.
- Suporte à autenticação e privacidade.
- Suporte à autoconfiguração.
- Suporte à seleção de rota.
- Suporte para tráfego com Qualidade de Serviço (QoS) garantida.

23.4 – INTERNET VIA REDE ELÉTRICA

Ainda são poucos os brasileiros que utilizam a internet via rede elétrica. Em São Paulo, primeira cidade em que a tecnologia BPL (Broadband Over Power Lines, em inglês) está disponível ao consumidor doméstico, ainda é pouco, mas os benefícios para esses consumidores são grandes, eventualmente, os futuros são evidentes.

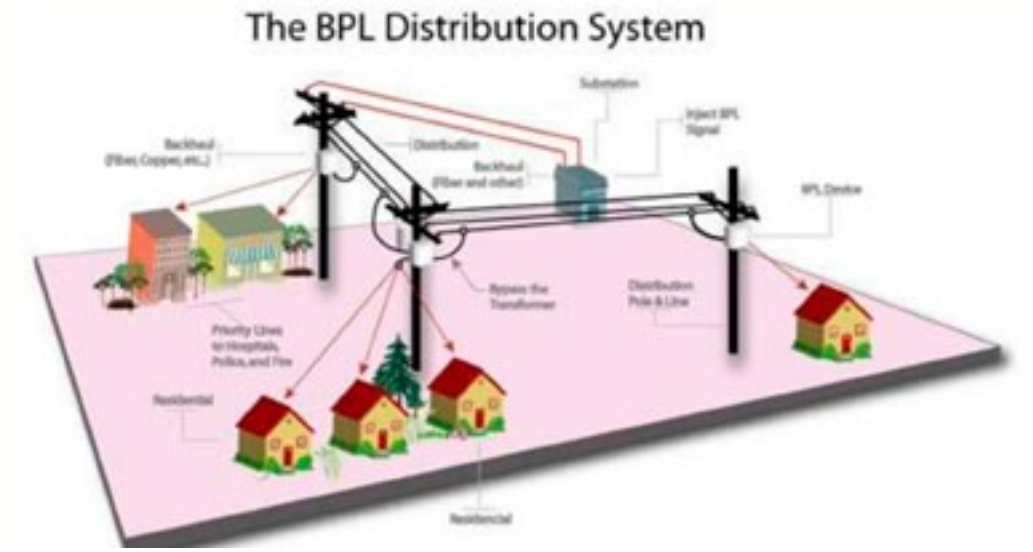

Figura 60 - Tecnologia BPL.
Fonte: http://2.bp.blogspot.com/_JnEmlSPBJdY/TBEphXNxbxI/AAAAAAAAAAY/eefQ9Va599g/s1600/plexeon-bpl-diagram-thumb1%2Bbrasil.jpg

23.5 – EXERCÍCIO PROPOSTO

1) Qual o novo protocolo de comunicação que surgiu após o IPv4? Cite suas melhorias.

_____
_____
_____

24 -PROJETO DE REDES

Neste capítulo falaremos um pouco sobre o futuro de projeto redes de computadores, seus requisitos e a sua utilização.

24.1 – INTRODUÇÃO

Podemos dizer que um projeto de redes de computadores é um estudo (ou planejamento) detalhado, destinado à criação de uma rede de computadores que possa satisfazer as necessidades de uma pessoa física ou jurídica, sendo o compartilhamento de informações e recursos, o objetivo mais comum.

24.2 – REQUISITOS

Para construir um projeto de redes, será necessário que se observem alguns requisitos essenciais para a construção do projeto proposto, tais como:

- **Funcionalidade:** a rede precisa funcionar, ela precisa permitir que os usuários desempenhem suas atividades profissionais e precisa oferecer conectividade de usuário para usuário e de usuário para aplicativo, com velocidade e confiabilidade razoáveis.
- **Escalabilidade:** a rede deve ser capaz de crescer. O projeto inicial deve ser ampliado sem causar grandes mudanças no projeto geral.
- **Adaptabilidade:** a rede precisa ser projetada com visão nas tecnologias futuras. A rede não deve incluir elementos que não permitam a implementação de novas tecnologias ao surgirem.
- **Gerenciabilidade:** a rede deve ser projetada de modo que fique fácil a sua monitoração e gerenciamento, para assegurar estabilidade permanente de operação.

24.3 – UTILIZAÇÃO

Para utilizar ao máximo a largura de banda disponível e o desempenho da rede local, devemos seguir as considerações no projeto de uma rede local, abordando as seguintes ideias:

- A função e colocação dos servidores.
- Questões de domínios de colisão.
- Questões de segmentação.
- Questões de domínios de broadcast.

24.4 – METODOLOGIA

Para que uma rede local seja eficiente e satisfaça às necessidades de seus usuários, ela deve ser projetada e implementada seguindo uma série planejada de etapas sistemáticas, tais como:

- Coletar requisitos e expectativas.
- Analisar requisitos e dados.
- Projetar a estrutura das camadas 1, 2 e 3 da rede local, ou seja, a topologia.
- Documentar a implementação física e lógica da rede.

O processo de coletar informações ajuda a esclarecer e a identificar quaisquer problemas atuais na rede. Essas informações incluem o histórico e o estado atual da organização,

projeções de crescimento, diretrizes operacionais e procedimentos de gerenciamento, sistemas e procedimentos burocráticos e as opiniões dos futuros usuários da rede local.

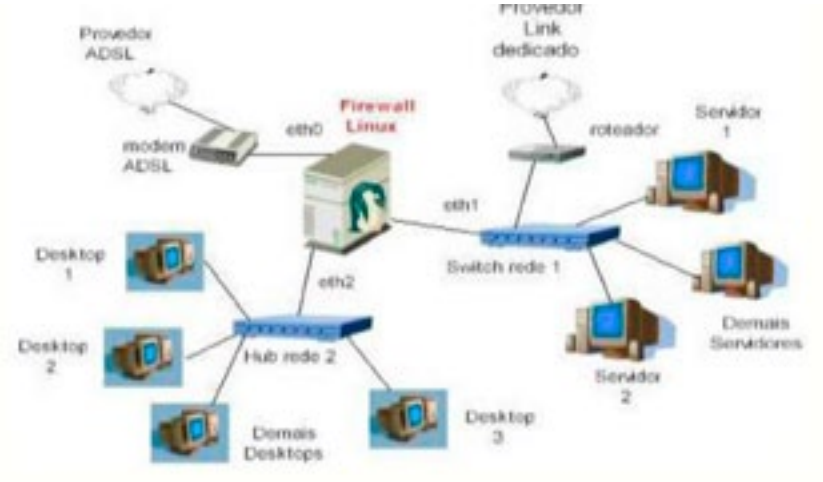

Figura 61 - Projeto de Redes.
Fonte: http://files.alissonferreira.webnode.com.pt/200000115-651c666169/rede.jpg

24.5 – EXERCÍCIOS PROPOSTOS

1) O que é Projeto de Rede?

_____
_____
_____

2) Quais os requisitos essenciais para um projeto de rede? Cite suas finalidades.

_____
_____
_____

REFERÊNCIAS

AMARAL, Allan Francisco Forzza. *Introdução a Redes de Computadores* – Colatina: CEaD/Ifes, 2010.

COUTINHO, Bruno Cardoso. *Redes TCP/IP* – Colatina: CEaD/Ifes, 2010.

Cracker. Disponível em: http://pt.wikipedia.org/wiki/Cracker. Acesso em: 22/08/2012.

Dispositivo de Ligação dos Componentes de Redes. Disponível em: http://www.slideshare.net/Taniabastos15/dispositivos-de-ligao-dos-componentes-rede. Acesso em: 22/08/2012.

FILIPPETTI, Marcos. Futuro da Internet – Artigo. Disponível em: http://www.projetoderedes.com.br/artigos/artigo_futuro_da_internet.php. Acesso em: 31/08/2012.

IDAPAC, Fundação. *Apostila de Redes.* p.52, 2005-2008.

JUNIOR, Frank J. Derfler. *Guia de Conectividade (Terceira Edição)*, Editora Campus.

MACHADO, Domingos Sávio Alcântara. *Política de Segurança - Workshop de Tecnologia da Informação*, 2001.

MARTINS, Marcelo Palmieri. *Redes Locais - UNIX x Windows NT.* Universidade Veiga de Almeida.

Modem. Disponível em: http://pt.wikipedia.org/wiki/Modem. Acesso em: 22/08/2012.

MORIMOTO, Carlos Eduardo. *Redes: Guia Prático.* Porto Alegre: Sul Editores, 2008.

PINHEIRO, José Maurício. *Guia Completo de Cabeamento de Redes*. Rio de Janeiro: Campus, 2003.

Redes Wan's. Disponível em: http://pt.wikipedia.org/wiki/Rede_de_longa_dist%C3%A2ncia. Acesso em: 22/08/2012.

SOARES, Luiz Fernando G.: *Redes locais*, Editora Campus, 1990.

TANENBAUM, Andrew S. *Redes de Computadores.* Traduzido por Vandenberg D. de Souza. Rio de Janeiro: Elsevier, 2003.

alfamacursos.com.br